CIS Oracle Linux 8 STIG Benchmark

v1.0.0 - 08-26-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Internal Only - General

Table of Contents

Terms of Use 1

Table of Contents 2

Overview 10

Target Technology Details 10

Intended Audience 10

Recommendation Definitions 11

Title 11

Assessment Status 11

Automated 11

Manual 11

Profile 11

Description 11

Rationale Statement 11

Audit Procedure 11

Remediation Procedure 12

Additional Information 12

Profile Definitions 13

Acknowledgements 14

Recommendations 15

1 STIG RULES 15

1.1 OL08-00-010000 (Manual) 16

1.2 OL08-00-010010 (Manual) 18

1.3 OL08-00-010019 (Manual) 20

1.4 OL08-00-010020 (Manual) 22

1.5 OL08-00-010030 (Manual) 25

1.6 OL08-00-010040 (Manual) 27

1.7 OL08-00-010050 (Manual) 31

1.8 OL08-00-010049 (Manual) 35

1.9 OL08-00-010060 (Manual) 38

1.10 OL08-00-010070 (Manual) 42

1.11 OL08-00-010090 (Manual) 44

1.12 OL08-00-010100 (Manual) 46

1.13 OL08-00-010110 (Manual) 47

1.14 OL08-00-010120 (Manual) 49

1.15 OL08-00-010121 (Manual) 50

1.16 OL08-00-010130 (Manual) 51

1.17 OL08-00-010140 (Manual) 53

1.18 OL08-00-010141 (Manual) 55

1.19 OL08-00-010149 (Manual) 57

1.20 OL08-00-010150 (Manual) 59

Internal Only - General

1.21 OL08-00-010151 (Manual) 61
1.22 OL08-00-010152 (Manual) 62
1.23 OL08-00-010159 (Manual) 63
1.24 OL08-00-010160 (Manual) 65
1.25 OL08-00-010161 (Manual) 67
1.26 OL08-00-010162 (Manual) 69
1.27 OL08-00-010163 (Manual) 71
1.28 OL08-00-010170 (Manual) 73
1.29 OL08-00-010171 (Manual) 75
1.30 OL08-00-010190 (Manual) 76
1.31 OL08-00-010200 (Manual) 78
1.32 OL08-00-010201 (Manual) 80
1.33 OL08-00-010210 (Manual) 82
1.34 OL08-00-010220 (Manual) 83
1.35 OL08-00-010230 (Manual) 84
1.36 OL08-00-010240 (Manual) 85
1.37 OL08-00-010250 (Manual) 86
1.38 OL08-00-010260 (Manual) 87
1.39 OL08-00-010287 (Manual) 88
1.40 OL08-00-010290 (Manual) 90
1.41 OL08-00-010291 (Manual) 92
1.42 OL08-00-010292 (Manual) 94
1.43 OL08-00-010293 (Manual) 96
1.44 OL08-00-010294 (Manual) 98
1.45 OL08-00-010295 (Manual) 100
1.46 OL08-00-010300 (Manual) 102
1.47 OL08-00-010310 (Manual) 103
1.48 OL08-00-010320 (Manual) 104
1.49 OL08-00-010330 (Manual) 105
1.50 OL08-00-010331 (Manual) 106
1.51 OL08-00-010340 (Manual) 107
1.52 OL08-00-010341 (Manual) 108
1.53 OL08-00-010350 (Manual) 109
1.54 OL08-00-010351 (Manual) 110
1.55 OL08-00-010358 (Manual) 111
1.56 OL08-00-010359 (Manual) 112
1.57 OL08-00-010360 (Manual) 114
1.58 OL08-00-010370 (Manual) 117
1.59 OL08-00-010371 (Manual) 119
1.60 OL08-00-010372 (Manual) 121
1.61 OL08-00-010373 (Manual) 124
1.62 OL08-00-010375 (Manual) 127
1.63 OL08-00-010376 (Manual) 129
1.64 OL08-00-010374 (Manual) 131
1.65 OL08-00-010379 (Manual) 134
1.66 OL08-00-010380 (Manual) 136
1.67 OL08-00-010381 (Manual) 138
1.68 OL08-00-010382 (Manual) 139
1.69 OL08-00-010383 (Manual) 140
1.70 OL08-00-010384 (Manual) 142
1.71 OL08-00-010385 (Manual) 144
1.72 OL08-00-010390 (Manual) 146
1.73 OL08-00-010400 (Manual) 148
1.74 OL08-00-010410 (Manual) 150
1.75 OL08-00-010420 (Manual) 151
1.76 OL08-00-010421 (Manual) 152

Internal Only - General

1.77 OL08-00-010422 (Manual) 154
1.78 OL08-00-010423 (Manual) 156
1.79 OL08-00-010424 (Manual) 158
1.80 OL08-00-010430 (Manual) 160
1.81 OL08-00-010440 (Manual) 162
1.82 OL08-00-010450 (Manual) 163
1.83 OL08-00-010460 (Manual) 165
1.84 OL08-00-010470 (Manual) 166
1.85 OL08-00-010472 (Manual) 167
1.86 OL08-00-010473 (Manual) 168
1.87 OL08-00-010480 (Manual) 170
1.88 OL08-00-010490 (Manual) 171
1.89 OL08-00-010500 (Manual) 172
1.90 OL08-00-010520 (Manual) 173
1.91 OL08-00-010521 (Manual) 175
1.92 OL08-00-010522 (Manual) 177
1.93 OL08-00-010540 (Manual) 179
1.94 OL08-00-010541 (Manual) 180
1.95 OL08-00-010542 (Manual) 181
1.96 OL08-00-010543 (Manual) 182
1.97 OL08-00-010544 (Manual) 183
1.98 OL08-00-010550 (Manual) 184
1.99 OL08-00-010561 (Manual) 186
1.100 OL08-00-010570 (Manual) 188
1.101 OL08-00-010571 (Manual) 190
1.102 OL08-00-010572 (Manual) 191
1.103 OL08-00-010580 (Manual) 192
1.104 OL08-00-010590 (Manual) 193
1.105 OL08-00-010600 (Manual) 195
1.106 OL08-00-010610 (Manual) 196
1.107 OL08-00-010620 (Manual) 197
1.108 OL08-00-010630 (Manual) 198
1.109 OL08-00-010640 (Manual) 199
1.110 OL08-00-010650 (Manual) 200
1.111 OL08-00-010660 (Manual) 201
1.112 OL08-00-010670 (Manual) 203
1.113 OL08-00-010671 (Manual) 205
1.114 OL08-00-010672 (Manual) 207
1.115 OL08-00-010673 (Manual) 209
1.116 OL08-00-010674 (Manual) 211
1.117 OL08-00-010675 (Manual) 213
1.118 OL08-00-010680 (Manual) 214
1.119 OL08-00-010690 (Manual) 216
1.120 OL08-00-010700 (Manual) 218
1.121 OL08-00-010710 (Manual) 219
1.122 OL08-00-010720 (Manual) 220
1.123 OL08-00-010730 (Manual) 221
1.124 OL08-00-010731 (Manual) 222
1.125 OL08-00-010740 (Manual) 224
1.126 OL08-00-010760 (Manual) 226
1.127 OL08-00-010750 (Manual) 227
1.128 OL08-00-010741 (Manual) 229
1.129 OL08-00-010780 (Manual) 231
1.130 OL08-00-010790 (Manual) 232
1.131 OL08-00-010770 (Manual) 233
1.132 OL08-00-010820 (Manual) 234

Internal Only - General

1.133 OL08-00-010800 (Manual) 236
1.134 OL08-00-010830 (Manual) 238
1.135 OL08-00-020000 (Manual) 239
1.136 OL08-00-020010 (Manual) 241
1.137 OL08-00-020011 (Manual) 244
1.138 OL08-00-020012 (Manual) 246
1.139 OL08-00-020013 (Manual) 249
1.140 OL08-00-020014 (Manual) 251
1.141 OL08-00-020015 (Manual) 254
1.142 OL08-00-020016 (Manual) 256
1.143 OL08-00-020017 (Manual) 259
1.144 OL08-00-020018 (Manual) 261
1.145 OL08-00-020019 (Manual) 264
1.146 OL08-00-020020 (Manual) 266
1.147 OL08-00-020021 (Manual) 269
1.148 OL08-00-020022 (Manual) 271
1.149 OL08-00-020023 (Manual) 274
1.150 OL08-00-020024 (Manual) 276
1.151 OL08-00-020025 (Manual) 278
1.152 OL08-00-020026 (Manual) 280
1.153 OL08-00-020027 (Manual) 282
1.154 OL08-00-020028 (Manual) 285
1.155 OL08-00-020030 (Manual) 288
1.156 OL08-00-020031 (Manual) 290
1.157 OL08-00-020032 (Manual) 292
1.158 OL08-00-020035 (Manual) 294
1.159 OL08-00-020043 (Manual) 295
1.160 OL08-00-020050 (Manual) 297
1.161 OL08-00-020060 (Manual) 299
1.162 OL08-00-020080 (Manual) 301
1.163 OL08-00-020081 (Manual) 304
1.164 OL08-00-020082 (Manual) 307
1.165 OL08-00-020090 (Manual) 310
1.166 OL08-00-020100 (Manual) 312
1.167 OL08-00-020101 (Manual) 314
1.168 OL08-00-020102 (Manual) 316
1.169 OL08-00-020103 (Manual) 318
1.170 OL08-00-020104 (Manual) 320
1.171 OL08-00-020110 (Manual) 322
1.172 OL08-00-020120 (Manual) 324
1.173 OL08-00-020130 (Manual) 326
1.174 OL08-00-020140 (Manual) 328
1.175 OL08-00-020150 (Manual) 330
1.176 OL08-00-020160 (Manual) 332
1.177 OL08-00-020170 (Manual) 334
1.178 OL08-00-020180 (Manual) 336
1.179 OL08-00-020190 (Manual) 337
1.180 OL08-00-020200 (Manual) 339
1.181 OL08-00-020210 (Manual) 341
1.182 OL08-00-020230 (Manual) 342
1.183 OL08-00-020231 (Manual) 344
1.184 OL08-00-020240 (Manual) 346
1.185 OL08-00-020250 (Manual) 348
1.186 OL08-00-020260 (Manual) 351
1.187 OL08-00-020261 (Manual) 353
1.188 OL08-00-020262 (Manual) 355

Internal Only - General

1.189 OL08-00-020263 (Manual) 356
1.190 OL08-00-020264 (Manual) 357
1.191 OL08-00-020270 (Manual) 358
1.192 OL08-00-020280 (Manual) 360
1.193 OL08-00-020290 (Manual) 362
1.194 OL08-00-020300 (Manual) 364
1.195 OL08-00-020310 (Manual) 365
1.196 OL08-00-020320 (Manual) 367
1.197 OL08-00-020330 (Manual) 369
1.198 OL08-00-020331 (Manual) 370
1.199 OL08-00-020332 (Manual) 371
1.200 OL08-00-020340 (Manual) 372
1.201 OL08-00-020350 (Manual) 373
1.202 OL08-00-020351 (Manual) 375
1.203 OL08-00-020352 (Manual) 376
1.204 OL08-00-020353 (Manual) 378
1.205 OL08-00-030000 (Manual) 380
1.206 OL08-00-030010 (Manual) 382
1.207 OL08-00-030020 (Manual) 384
1.208 OL08-00-030030 (Manual) 386
1.209 OL08-00-030040 (Manual) 388
1.210 OL08-00-030060 (Manual) 390
1.211 OL08-00-030061 (Manual) 392
1.212 OL08-00-030062 (Manual) 393
1.213 OL08-00-030063 (Manual) 395
1.214 OL08-00-030070 (Manual) 397
1.215 OL08-00-030080 (Manual) 399
1.216 OL08-00-030090 (Manual) 401
1.217 OL08-00-030100 (Manual) 403
1.218 OL08-00-030110 (Manual) 405
1.219 OL08-00-030120 (Manual) 407
1.220 OL08-00-030121 (Manual) 409
1.221 OL08-00-030122 (Manual) 411
1.222 OL08-00-030130 (Manual) 413
1.223 OL08-00-030140 (Manual) 416
1.224 OL08-00-030150 (Manual) 420
1.225 OL08-00-030160 (Manual) 423
1.226 OL08-00-030170 (Manual) 426
1.227 OL08-00-030171 (Manual) 429
1.228 OL08-00-030172 (Manual) 432
1.229 OL08-00-030180 (Manual) 435
1.230 OL08-00-030181 (Manual) 439
1.231 OL08-00-030190 (Manual) 445
1.232 OL08-00-030200 (Manual) 448
1.233 OL08-00-030250 (Manual) 451
1.234 OL08-00-030260 (Manual) 454
1.235 OL08-00-030280 (Manual) 457
1.236 OL08-00-030290 (Manual) 460
1.237 OL08-00-030300 (Manual) 463
1.238 OL08-00-030301 (Manual) 466
1.239 OL08-00-030302 (Manual) 469
1.240 OL08-00-030310 (Manual) 472
1.241 OL08-00-030311 (Manual) 475
1.242 OL08-00-030312 (Manual) 477
1.243 OL08-00-030313 (Manual) 480
1.244 OL08-00-030314 (Manual) 482

Internal Only - General

1.245 OL08-00-030315 (Manual) 484
1.246 OL08-00-030316 (Manual) 486
1.247 OL08-00-030317 (Manual) 489
1.248 OL08-00-030320 (Manual) 492
1.249 OL08-00-030330 (Manual) 495
1.250 OL08-00-030340 (Manual) 498
1.251 OL08-00-030350 (Manual) 501
1.252 OL08-00-030360 (Manual) 504
1.253 OL08-00-030361 (Manual) 507
1.254 OL08-00-030370 (Manual) 510
1.255 OL08-00-030390 (Manual) 513
1.256 OL08-00-030400 (Manual) 516
1.257 OL08-00-030410 (Manual) 519
1.258 OL08-00-030420 (Manual) 522
1.259 OL08-00-030480 (Manual) 526
1.260 OL08-00-030490 (Manual) 529
1.261 OL08-00-030550 (Manual) 532
1.262 OL08-00-030560 (Manual) 535
1.263 OL08-00-030570 (Manual) 538
1.264 OL08-00-030580 (Manual) 541
1.265 OL08-00-030590 (Manual) 544
1.266 OL08-00-030600 (Manual) 547
1.267 OL08-00-030601 (Manual) 550
1.268 OL08-00-030602 (Manual) 553
1.269 OL08-00-030603 (Manual) 556
1.270 OL08-00-030610 (Manual) 557
1.271 OL08-00-030620 (Manual) 558
1.272 OL08-00-030630 (Manual) 560
1.273 OL08-00-030640 (Manual) 562
1.274 OL08-00-030650 (Manual) 564
1.275 OL08-00-030660 (Manual) 566
1.276 OL08-00-030670 (Manual) 568
1.277 OL08-00-030680 (Manual) 570
1.278 OL08-00-030690 (Manual) 572
1.279 OL08-00-030700 (Manual) 574
1.280 OL08-00-030710 (Manual) 576
1.281 OL08-00-030720 (Manual) 578
1.282 OL08-00-030730 (Manual) 580
1.283 OL08-00-030731 (Manual) 582
1.284 OL08-00-030740 (Manual) 584
1.285 OL08-00-030741 (Manual) 586
1.286 OL08-00-030742 (Manual) 588
1.287 OL08-00-040000 (Manual) 590
1.288 OL08-00-040001 (Manual) 592
1.289 OL08-00-040002 (Manual) 594
1.290 OL08-00-040004 (Manual) 596
1.291 OL08-00-040010 (Manual) 598
1.292 OL08-00-040020 (Manual) 600
1.293 OL08-00-040021 (Manual) 603
1.294 OL08-00-040022 (Manual) 605
1.295 OL08-00-040023 (Manual) 607
1.296 OL08-00-040024 (Manual) 609
1.297 OL08-00-040025 (Manual) 611
1.298 OL08-00-040026 (Manual) 613
1.299 OL08-00-040030 (Manual) 615
1.300 OL08-00-040070 (Manual) 617

Internal Only - General

1.301 OL08-00-040080 (Manual) 619
1.302 OL08-00-040090 (Manual) 621
1.303 OL08-00-040100 (Manual) 623
1.304 OL08-00-040101 (Manual) 625
1.305 OL08-00-040110 (Manual) 627
1.306 OL08-00-040111 (Manual) 629
1.307 OL08-00-040120 (Manual) 632
1.308 OL08-00-040121 (Manual) 634
1.309 OL08-00-040122 (Manual) 636
1.310 OL08-00-040123 (Manual) 638
1.311 OL08-00-040124 (Manual) 640
1.312 OL08-00-040125 (Manual) 642
1.313 OL08-00-040126 (Manual) 644
1.314 OL08-00-040127 (Manual) 646
1.315 OL08-00-040128 (Manual) 648
1.316 OL08-00-040129 (Manual) 650
1.317 OL08-00-040130 (Manual) 652
1.318 OL08-00-040131 (Manual) 654
1.319 OL08-00-040132 (Manual) 656
1.320 OL08-00-040133 (Manual) 658
1.321 OL08-00-040134 (Manual) 660
1.322 OL08-00-040135 (Manual) 662
1.323 OL08-00-040136 (Manual) 664
1.324 OL08-00-040137 (Manual) 666
1.325 OL08-00-040139 (Manual) 669
1.326 OL08-00-040140 (Manual) 671
1.327 OL08-00-040141 (Manual) 673
1.328 OL08-00-040150 (Manual) 675
1.329 OL08-00-040159 (Manual) 677
1.330 OL08-00-040160 (Manual) 679
1.331 OL08-00-040161 (Manual) 681
1.332 OL08-00-040170 (Manual) 682
1.333 OL08-00-040171 (Manual) 683
1.334 OL08-00-040172 (Manual) 685
1.335 OL08-00-040180 (Manual) 686
1.336 OL08-00-040190 (Manual) 688
1.337 OL08-00-040200 (Manual) 689
1.338 OL08-00-040209 (Manual) 690
1.339 OL08-00-040210 (Manual) 692
1.340 OL08-00-040220 (Manual) 694
1.341 OL08-00-040230 (Manual) 696
1.342 OL08-00-040239 (Manual) 698
1.343 OL08-00-040240 (Manual) 700
1.344 OL08-00-040249 (Manual) 702
1.345 OL08-00-040250 (Manual) 704
1.346 OL08-00-040259 (Manual) 706
1.347 OL08-00-040260 (Manual) 708
1.348 OL08-00-040261 (Manual) 710
1.349 OL08-00-040262 (Manual) 712
1.350 OL08-00-040270 (Manual) 714
1.351 OL08-00-040279 (Manual) 716
1.352 OL08-00-040280 (Manual) 718
1.353 OL08-00-040281 (Manual) 720
1.354 OL08-00-040282 (Manual) 722
1.355 OL08-00-040283 (Manual) 724
1.356 OL08-00-040284 (Manual) 726

Internal Only - General

1.357 OL08-00-040285 (Manual) 728
1.358 OL08-00-040286 (Manual) 730
1.359 OL08-00-040290 (Manual) 732
1.360 OL08-00-040300 (Manual) 733
1.361 OL08-00-040310 (Manual) 735
1.362 OL08-00-040320 (Manual) 737
1.363 OL08-00-040321 (Manual) 738
1.364 OL08-00-040330 (Manual) 739
1.365 OL08-00-040340 (Manual) 740
1.366 OL08-00-040341 (Manual) 742
1.367 OL08-00-040342 (Manual) 744
1.368 OL08-00-040350 (Manual) 746
1.369 OL08-00-040360 (Manual) 747
1.370 OL08-00-040370 (Manual) 748
1.371 OL08-00-040380 (Manual) 749
1.372 OL08-00-040390 (Manual) 750
1.373 OL08-00-040400 (Manual) 751

Appendix: Summary Table 753

Appendix: Change History 771

Internal Only - General

Overview

Target Technology Details

Oracle Linux 8 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Oracle Linux 8 and are looking to comply with the STIG guidance

Internal Only - General

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Internal Only - General

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Internal Only - General

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Internal Only - General

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Oracle Linux 8

Internal Only - General

Recommendations

1 STIG RULES

Oracle Linux 8

Oracle Linux 8 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

Internal Only - General

1.1 OL08-00-010000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must be a vendor-supported release.

```
GROUP ID: V-248521
RULE ID: SV-248521r991589
```

Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the version of the operating system is vendor supported.

Check the version of the operating system with the following command:

```
$ sudo cat /etc/oracle-release
```

Oracle Linux Server release 8.2

Current End of Premier Support for Oracle Linux 8 is July 2029, while Extended Support might consider an extended term.

If the release is not supported by the vendor, this is a finding.

Remediation:

Upgrade to a supported version of the operating system.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.2 OL08-00-010010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 vendor-packaged system security patches and updates must be installed and up to date.

```
GROUP ID: V-248523
RULE ID: SV-248523r991589
```

Rationale:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals.

New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Internal Only - General

Audit:

Verify the operating system security patches and updates are installed and up to date. Updates are required to be applied with a frequency determined by the site or Program Management Office (PMO).

Obtain the list of available package security updates from Oracle. The URL for updates is https://linux.oracle.com/errata/. It is important to note that updates provided by Oracle may not be present on the system if the underlying packages are not installed.

Check that the available package security updates have been installed on the system with the following command:

```
$ sudo yum history list | more

Loaded plugins: langpacks, product-id, subscription-manager
ID | Command line | Date and time | Action(s) | Altered
-------------------------------------------------------------------------------
--
70 | install aide | 2020-03-05 10:58 | Install | 1
69 | update -y | 2020-03-04 14:34 | Update | 18 EE
68 | install vlc | 2020-02-21 17:12 | Install | 21
67 | update -y | 2020-02-21 17:04 | Update | 7 EE
```

If package updates have not been performed on the system within the timeframe that the site/program documentation requires, this is a finding.

Typical update frequency may be overridden by Information Assurance Vulnerability Alert (IAVA) notifications from CYBERCOM.

If the operating system is not in compliance with the Information Assurance Vulnerability Management (IAVM) process, this is a finding.

Remediation:

Install the operating system patches or updated packages available from Oracle within 30 days or sooner as local policy dictates.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.3 OL08-00-010019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must ensure cryptographic verification of vendor software packages.

```
GROUP ID: V-256978
RULE ID: SV-256978r1015073
```

Rationale:

Cryptographic verification of vendor software packages ensures that all software packages are obtained from a valid source and protects against spoofing that could lead to installation of malware on the system. Oracle cryptographically signs all software packages, which includes updates, with a GPG key to verify that they are valid.

Audit:

Confirm Oracle package-signing key is installed on the system and verify its fingerprint matches vendor value.

Note: The GPG key is defined in key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-oracle" by default.

List Oracle GPG keys installed on the system:

```
 $ sudo rpm -q --queryformat "%{SUMMARY}\n" gpg-pubkey | grep -i "oracle"

 gpg(Oracle OSS group (Open Source Software group) <build@oss.oracle.com>)
```

If Oracle GPG key is not installed, this is a finding.

List key fingerprint of installed Oracle GPG key:

```
 $ sudo gpg -q --keyid-format short --with-fingerprint /etc/pki/rpm-gpg/RPM-
GPG-KEY-oracle
```

If key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-oracle" is missing, this is a finding.

Example output:

```
 pub   rsa4096/AD986DA3 2019-04-09 [SC] [expires: 2039-04-04]
       Key fingerprint = 76FD 3DB1 3AB6 7410 B89D  B10E 8256 2EA9 AD98 6DA3
 uid   Oracle OSS group (Open Source Software group) <build@oss.oracle.com>
 sub   rsa4096/D95DC12B 2019-04-09 [E] [expires: 2039-04-04]
```

Compare key fingerprint of installed Oracle GPG key with fingerprint listed for OL 8 on Oracle verification webpage at https://linux.oracle.com/security/gpg/#gpg.

If key fingerprint does not match, this is a finding.

Internal Only - General

Remediation:

Install Oracle package-signing key on the system and verify its fingerprint matches vendor value.

Insert OL 8 installation disc or attach OL 8 installation image to the system. Mount the disc or image to make the contents accessible inside the system.

Assuming the mounted location is "/media/cdrom", use the following command to copy Oracle GPG key file onto the system:

```
$ sudo cp /media/cdrom/RPM-GPG-KEY-oracle /etc/pki/rpm-gpg/
```

Import Oracle GPG keys from key file into system keyring:

```
$ sudo rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
```

Using the steps listed in the Check Text, confirm the newly imported key shows as installed on the system and verify its fingerprint matches vendor value.

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

Internal Only - General

1.4 OL08-00-010020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must implement NIST FIPS-validated cryptography for the following: To provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

```
GROUP ID: V-248524
RULE ID: SV-248524r1069154
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

OL 8 uses GRUB 2 as the default bootloader. Note that GRUB 2 command-line parameters are defined in the "kernelopts" variable of the "/boot/grub2/grubenv" file for all kernel boot entries. The command "fips-mode-setup" modifies the "kernelopts" variable, which in turn updates all kernel boot entries.

The fips=1 kernel option needs to be added to the kernel command line during system installation so that key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users must also ensure the system has plenty of entropy during the installation process by moving the mouse around, or if no mouse is available, ensuring that many keystrokes are typed. The recommended amount of keystrokes is 256 and more. Less than 256 keystrokes may generate a nonunique key.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000423-GPOS-00187

Internal Only - General

Audit:

Verify the operating system implements DOD-approved encryption to protect the confidentiality of remote access sessions.

Check to see if FIPS mode is enabled with the following command:

```
$ fips-mode-setup --check

FIPS mode is enabled
```

If FIPS mode is "enabled", check if the kernel boot parameter is configured for FIPS mode with the following command:

```
$ sudo grub2-editenv list | grep fips

kernelopts=...fips=1
```

If the kernel boot parameter is configured to use FIPS mode, check to see if the system is in FIPS mode with the following command:

```
$ sudo cat /proc/sys/crypto/fips_enabled

1
```

If FIPS mode is not "enabled", the kernel boot parameter is not configured for FIPS mode, or the system does not have a value of "1" for "fips_enabled" in "/proc/sys/crypto", this is a finding.

Remediation:

Configure the operating system to implement DOD-approved encryption by following the steps below:

To enable strict FIPS compliance, the fips=1 kernel option must be added to the kernel boot parameters during system installation so key generation is done with FIPS-approved algorithms and continuous monitoring tests in place.

Enable FIPS mode after installation (not strict FIPS-compliant) with the following command:

```
$ sudo fips-mode-setup --enable
```

Reboot the system for the changes to take effect.

Internal Only - General

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

Internal Only - General

1.5 OL08-00-010030 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

All OL 8 local disk partitions must implement cryptographic mechanisms to prevent unauthorized disclosure or modification of all information that requires at-rest protection.

```
GROUP ID: V-248525
RULE ID: SV-248525r1016496
```

Rationale:

OL 8 systems handling data requiring "data-at-rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Audit:

Verify OL 8 prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

If there is a documented and approved reason for not having data-at-rest encryption at the operating system level, such as encryption provided by a hypervisor or a disk storage array in a virtualized environment, this requirement is not applicable.

Verify all system partitions are encrypted with the following command:

```
 $ sudo blkid

 /dev/mapper/ol-root:  UUID="67b7d7fe-de60-6fd0-befb-e6748cf97743"
TYPE="crypto_LUKS"
```

Every persistent disk partition present must be of type "crypto_LUKS".

If any partitions other than the boot partition or pseudo file systems (such as "/proc" or "/sys") are not listed, ask the administrator to indicate how the partitions are encrypted. If there is no evidence that these partitions are encrypted, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to prevent unauthorized modification of all information at rest by using disk encryption.

Encrypting a partition in an already-installed system is more difficult because existing partitions will need to be resized and changed.

To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

Internal Only - General

1.6 OL08-00-010040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system via an SSH logon.

```
GROUP ID: V-248526
RULE ID: SV-248526r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-
authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following
conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but
not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel
misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine
monitoring, interception, and search, and may be disclosed or used for any USG-authorized
purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG
interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI
investigative searching or monitoring of the content of privileged communications, or work
product, related to personal representation or services by attorneys, psychotherapists, or
clergy, and their assistants. Such communications and work product are private and confidential.
See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of
characters that can be displayed in the banner:


"I've read & consent to terms in IS user agreem't."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Internal Only - General

Audit:

Verify that any publicly accessible connection to the operating system displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the system.

Check for the location of the banner file being used with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*banner'

banner /etc/issue
```

This command will return the banner keyword and the name of the file that contains the SSH banner (in this case "/etc/issue").

If the line is commented out, this is a finding.

If conflicting results are returned, this is a finding.

View the file specified by the banner keyword to check that it matches the text of the Standard Mandatory DOD Notice and Consent Banner:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

If the system does not display a graphical logon banner or the banner does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

If the text in the file does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via the SSH.

Edit the "/etc/ssh/sshd_config" file to uncomment the banner keyword and configure it to point to a file that will contain the logon banner (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). An example configuration line is:

```
banner /etc/issue
```

Either create the file containing the banner or replace the text in the file with the Standard Mandatory DOD Notice and Consent Banner. The DOD-required text is:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

The SSH service must be restarted for changes to take effect.

Internal Only - General

Additional Information:
CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

Internal Only - General

1.7 OL08-00-010050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

```
GROUP ID: V-248528
RULE ID: SV-248528r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to
routine monitoring, interception, and search, and may be disclosed or used for any
USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to
protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or
CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or services by
attorneys, psychotherapists, or clergy, and their assistants. Such communications
and work product are private and confidential. See User Agreement for details."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Internal Only - General

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify OL 8 displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon.

Check that the operating system displays the exact Standard Mandatory DoD Notice and Consent Banner text with the command:

```
$ sudo grep banner-message-text /etc/dconf/db/local.d/*
banner-message-text=
'You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.\nBy using this IS (which includes any
device attached to this IS), you consent to the following conditions:\n-The
USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations.\n-At any time, the USG may
inspect and seize data stored on this IS.\n-Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose.\n-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal benefit or
privacy.\n-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of the content
of privileged communications, or work product, related to personal
representation or services by attorneys, psychotherapists, or clergy, and
their assistants. Such communications and work product are private and
confidential. See User Agreement for details. '
```

Note: The "\n" characters are for formatting only. They will not be displayed on the graphical interface.

If the banner does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable.

Add the following lines to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

```
banner-message-text='You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\n-The USG routinely intercepts and monitors communications on
this IS for purposes including, but not limited to, penetration testing,
COMSEC monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.\n-At any
time, the USG may inspect and seize data stored on this IS.\n-Communications
using, or data stored on, this IS are not private, are subject to routine
monitoring, interception, and search, and may be disclosed or used for any
USG-authorized purpose.\n-This IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\n-Notwithstanding the above, using this IS does
not constitute consent to PM, LE or CI investigative searching or monitoring
of the content of privileged communications, or work product, related to
personal representation or services by attorneys, psychotherapists, or
clergy, and their assistants. Such communications and work product are
private and confidential. See User Agreement for details. '
```

Note: The "\n" characters are for formatting only. They will not be displayed on the graphical interface.

Run the following command to update the database:

```
$ sudo dconf update
```


Internal Only - General

Additional Information:
CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

Internal Only - General

1.8 OL08-00-010049 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must display a banner before granting local or remote access to the system via a graphical user logon.

```
GROUP ID: V-248527
RULE ID: SV-248527r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify OL 8 displays a banner before granting access to the operating system via a graphical user logon.

Determine if the operating system displays a banner at the logon screen with the following command:

```
$ sudo grep banner-message-enable /etc/dconf/db/local.d/*

banner-message-enable=true
```

If "banner-message-enable" is set to "false" or is missing, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to display a banner before granting access to the system.

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable.

Create a database to contain the system-wide graphical user logon settings (if it does not already exist) with the following command:

```
$ sudo touch /etc/dconf/db/local.d/01-banner-message
```

Add the following lines to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

```
[org/gnome/login-screen]

banner-message-enable=true
```

Run the following command to update the database:

```
$ sudo dconf update
```


Internal Only - General

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

Internal Only - General

1.9 OL08-00-010060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

```
GROUP ID: V-248529
RULE ID: SV-248529r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to
the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to
routine monitoring, interception, and search, and may be disclosed or used for any
USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to
protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or
CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or services by
attorneys, psychotherapists, or clergy, and their assistants. Such communications
and work product are private and confidential. See User Agreement for details."
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Internal Only - General

Audit:

Verify OL 8 displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon.

Check that OL 8 displays a banner at the command line login screen with the following command:

```
$ sudo cat /etc/issue
```

If the banner is set correctly, it will return the following text:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent
to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

If the banner text does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via command line logon.

Edit the "/etc/issue" file to replace the default text with the Standard Mandatory DoD Notice and Consent Banner. The DoD-required text is:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent
to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests -- not for your personal benefit or
privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```


Internal Only - General

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

Internal Only - General

1.10 OL08-00-010070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 remote access methods must be monitored.

```
GROUP ID: V-248530
RULE ID: SV-248530r958406
```

Rationale:

Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyberattacks and ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that OL 8 monitors all remote access methods.

Check that remote access methods are being logged by running the following command:

```
$ sudo grep -E '(auth\.\*|authpriv\.\*|daemon\.\*)' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf

/etc/rsyslog.conf:auth.*;authpriv.*;daemon.* /var/log/secure
```

If "auth.*", "authpriv.*", or "daemon.*" are not configured to be logged, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to monitor all remote access methods by installing rsyslog with the following command:

```
$ sudo yum install rsyslog
```

Add or update the following lines to the "/etc/rsyslog.conf" file:

```
auth.*;authpriv.*;daemon.* /var/log/secure
```

The "rsyslog" service must be restarted for the changes to take effect. To restart the "rsyslog" service, run the following command:

```
$ sudo systemctl restart rsyslog.service
```

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

Internal Only - General

1.11 OL08-00-010090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

```
GROUP ID: V-248531
RULE ID: SV-248531r1015027
```

Rationale:

Without path validation, the relying party cannot make an informed trust decision when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000384-GPOS-00167

Internal Only - General

Audit:

Verify OL 8, for PKI-based authentication, has valid certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Note: If the system administrator (SA) demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.

Check that the system has a valid DOD root CA installed with the following command:

```
$ sudo openssl x509 -text -in /etc/sssd/pki/sssd_auth_ca_db.pem

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3
Validity
Not Before: Mar 20 18:46:41 2012 GMT
Not After : Dec 30 18:46:41 2029 GMT
Subject: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
```

If the root ca file is not a DOD-issued certificate with a valid date installed in the "/etc/sssd/pki/sssd_auth_ca_db.pem" location, this is a finding.

Remediation:

Configure OL 8, for PKI-based authentication, to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Obtain a valid copy of the DOD root CA file from the PKI CA certificate bundle at cyber.mil and copy it into the following file:

```
/etc/sssd/pki/sssd_auth_ca_db.pem
```

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5::IA-5 (2) (b) (2)

CCI-001991 The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

- NIST SP 800-53 Revision 4::IA-5 (2) (d)

Internal Only - General

1.12 OL08-00-010100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8, for certificate-based authentication, must enforce authorized access to the corresponding private key.

```
GROUP ID: V-248532
RULE ID: SV-248532r958450
```

Rationale:

If an unauthorized user obtains access to a private key without a passcode, that user would have unauthorized access to any system where the associated public key has been installed.

Audit:

Verify the SSH private key files have a passcode.

For each private key stored on the system, use the following command:

```
$ sudo ssh-keygen -y -f /path/to/file
```

If the contents of the key are displayed, this is a finding.

Remediation:

Create a new private and public key pair that uses a passcode with the following command:

```
$ sudo ssh-keygen -n [passphrase]
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

Internal Only - General

1.13 OL08-00-010110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

```
GROUP ID: V-248533
RULE ID: SV-248533r1015028
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DOD data may be compromised.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DOD requirements.

Audit:

Verify that the shadow password suite configuration is set to encrypt passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

Check the hashing algorithm that is being used to hash passwords with the following command:

```
$ sudo cat /etc/login.defs | grep -i crypt

ENCRYPT_METHOD SHA512
```

If "ENCRYPT_METHOD" does not equal SHA512 or greater, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to encrypt all stored passwords.

Edit/modify the following line in the "/etc/login.defs" file and set "[ENCRYPT_METHOD]" to SHA512:

```
ENCRYPT_METHOD SHA512
```

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)

Internal Only - General

1.14 OL08-00-010120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must employ FIPS 140-2 approved cryptographic hashing algorithms for all stored passwords.

```
GROUP ID: V-248534
RULE ID: SV-248534r1015029
```

Rationale:

The system must use a strong hashing algorithm to store the password.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

Confirm that the interactive user account passwords are using a strong password hash with the following command:

```
$ sudo cut -d: -f2 /etc/shadow

$6$kcOnRq/5$NUEYPuyL.wghQwWssXRcLRFiiru7f5JPV6GaJhNC2aK5F3PZpE/BCCtwrxRc/AInK
MNX3CdMw11m9STiql12f/
```

Password hashes "!" or "*" indicate inactive accounts not available for logon and are not evaluated.

If any interactive user password hash does not begin with "6", this is a finding.

Remediation:

Lock all interactive user accounts not using SHA-512 hashing until the passwords can be regenerated with SHA-512.

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)

Internal Only - General

1.15 OL08-00-010121 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The OL 8 operating system must not have accounts configured with blank or null passwords.

```
GROUP ID: V-252650
RULE ID: SV-252650r991589
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

Check the "/etc/shadow" file for blank passwords with the following command:

```
$ sudo awk -F: '!$2 {print $1}' /etc/shadow
```

If the command returns any results, this is a finding.

Remediation:

Configure all accounts on the system to have a password or lock the account with the following commands:

Perform a password reset:

```
$ sudo passwd [username]
```

Lock an account:

```
$ sudo passwd -l [username]
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.16 OL08-00-010130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 shadow password suite must be configured to use a sufficient number of hashing rounds.

```
GROUP ID: V-248535
RULE ID: SV-248535r1044786
```

Rationale:

The system must use a strong hashing algorithm to store the password. The system must use a sufficient number of hashing rounds to ensure the required level of entropy.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Audit:

Check that a minimum number of hash rounds is configured by running the following command:

```
 $ sudo grep -E "^SHA_CRYPT_" /etc/login.defs
```

If only one of "SHA_CRYPT_MIN_ROUNDS" or "SHA_CRYPT_MAX_ROUNDS" is set, and this value is below "100000", this is a finding.

If both "SHA_CRYPT_MIN_ROUNDS" and "SHA_CRYPT_MAX_ROUNDS" are set, and the value for either is below "100000", this is a finding.

Remediation:

Configure OL 8 to encrypt all stored passwords with a strong cryptographic hash.

Edit/modify the following line in the "/etc/login.defs" file and set "SHA_CRYPT_MIN_ROUNDS" to a value no lower than "100000":

```
SHA_CRYPT_MIN_ROUNDS 100000
```


Internal Only - General

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)

Internal Only - General

1.17 OL08-00-010140 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 operating systems booted with United Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user mode and maintenance.

```
GROUP ID: V-248537
RULE ID: SV-248537r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for OL 8 and is designed to require a password to boot into single-user mode or modify the boot menu.

Audit:

For systems that use BIOS, this is not applicable.

Determine if an encrypted password is set for the grub superusers account. On systems that use UEFI, use the following command:

```
$ sudo grep -iw grub2_password /boot/efi/EFI/redhat/user.cfg

GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the grub superusers account password does not begin with "grub.pbkdf2.sha512", this is a finding.

Remediation:

Configure the system to require an encrypted grub bootloader password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the "/boot/efi/EFI/redhat/user.cfg" file.

Generate an encrypted grub2 password for the grub superusers account with the following command:

```
$ sudo grub2-setpassword

Enter password:
Confirm password:
```


Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.18 OL08-00-010141 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 operating systems booted with United Extensible Firmware Interface (UEFI) must have a unique name for the grub superusers account when booting into single-user mode and maintenance.

```
GROUP ID: V-248538
RULE ID: SV-248538r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for OL 8 and is designed to require a password to boot into single-user mode or modify the boot menu. The GRUB 2 superuser account is an account of last resort. Establishing a unique username for this account hardens the boot loader against brute force attacks. Due to the nature of the superuser account database being distinct from the OS account database, this allows the use of a username that is not among those within the OS account database. Examples of non-unique superusers names are (root, superuser, unlock, etc.)

Audit:

For systems that use BIOS, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
$ sudo grep -iw "superusers" /boot/efi/EFI/redhat/grub.cfg

set superusers="[someuniqueUserNamehere]"
export superusers
```

If "superusers" is identical to any OS account name or is missing a name, this is a finding.

Internal Only - General

Remediation:

Configure the system to replace "root" with a unique name for the grub superusers account.

Edit the /etc/grub.d/01_users file and add or modify the following lines:

```
set superusers="[someuniqueUserNamehere]"
export superusers
password_pbkdf2 [someuniqueUserNamehere] ${GRUB2_PASSWORD}
```

Generate a new grub.cfg file with the following command:

```
$ sudo grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.19 OL08-00-010149 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 operating systems booted with a BIOS must have a unique name for the grub superusers account when booting into single-user and maintenance modes.

```
GROUP ID: V-248539
RULE ID: SV-248539r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for OL 8 and is designed to require a password to boot into single-user mode or modify the boot menu. The GRUB 2 superuser account is an account of last resort. Establishing a unique username for this account hardens the boot loader against brute force attacks. Due to the nature of the superuser account database being distinct from the OS account database, this allows the use of a username that is not among those within the OS account database. Examples of non-unique superusers names are (root, superuser, unlock, etc.)

Audit:

For systems that use UEFI, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
$ sudo grep -iw "superusers" /boot/grub2/grub.cfg

set superusers="[someuniqueUserNamehere]"
export superusers
```

If "superusers" is identical to any OS account name or is missing a name, this is a finding.

Internal Only - General

Remediation:

Configure the system to replace "root" with a unique name for the grub superusers account.

Edit the /etc/grub.d/01_users file and add or modify the following lines:

```
set superusers="[someuniqueUserNamehere]"
export superusers
password_pbkdf2 [someuniqueUserNamehere] ${GRUB2_PASSWORD}
```

Generate a new grub.cfg file with the following command:

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.20 OL08-00-010150 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 operating systems booted with a BIOS must require authentication upon booting into single-user and maintenance modes.

```
GROUP ID: V-248540
RULE ID: SV-248540r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for OL 8 and is designed to require a password to boot into single-user mode or modify the boot menu.

Audit:

For systems that use UEFI, this is not applicable.

Determine if an encrypted password is set for the grub superusers account. On systems that use a BIOS, use the following command:

```
$ sudo grep -iw grub2_password /boot/grub2/user.cfg

GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the grub superusers account password does not begin with "grub.pbkdf2.sha512", this is a finding.

Remediation:

Configure the system to require a grub bootloader password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the "/boot/grub2/user.cfg" file.

Generate an encrypted grub2 password for the grub superusers account with the following command:

```
$ sudo grub2-setpassword

Enter password:
Confirm password:
```


Internal Only - General

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.21 OL08-00-010151 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 operating systems must require authentication upon booting into rescue mode.

```
GROUP ID: V-248541
RULE ID: SV-248541r958472
```

Rationale:

If the system does not require valid root authentication before it boots into emergency or rescue mode, anyone who invokes emergency or rescue mode is granted privileged access to all files on the system.

Audit:

Determine if the system requires authentication for rescue mode with the following command:

```
$ sudo grep sulogin-shell /usr/lib/systemd/system/rescue.service

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

If the "ExecStart" line is configured for anything other than "/usr/lib/systemd/systemd-sulogin-shell rescue" or is commented out or missing, this is a finding.

Remediation:

Configure the system to require authentication upon booting into rescue mode by adding the following line to the "/usr/lib/systemd/system/rescue.service" file:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.22 OL08-00-010152 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 operating systems must require authentication upon booting into emergency mode.

```
GROUP ID: V-248542
RULE ID: SV-248542r958472
```

Rationale:

If the system does not require valid root authentication before it boots into emergency or rescue mode, anyone who invokes emergency or rescue mode is granted privileged access to all files on the system.

Audit:

Determine if the system requires authentication for emergency mode with the following command:

```
$ sudo grep sulogin-shell /usr/lib/systemd/system/emergency.service

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

If the "ExecStart" line is configured for anything other than "/usr/lib/systemd/systemd-sulogin-shell emergency" or is commented out or missing, this is a finding.

Remediation:

Configure the system to require authentication upon booting into emergency mode by adding the following line to the "/usr/lib/systemd/system/emergency.service" file:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

Internal Only - General

1.23 OL08-00-010159 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "pam_unix.so" module must be configured in the system-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.

```
GROUP ID: V-248543
RULE ID: SV-248543r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

OL 8 systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify that the "pam_unix.so" module is configured to use sha512.

Check that pam_unix.so module is configured to use sha512 in /etc/pam.d/system-auth with the following command:

```
$ sudo grep password /etc/pam.d/system-auth | grep pam_unix

password sufficient pam_unix.so sha512
```

If "sha512" is missing, or is commented out, this is a finding.

Remediation:

Configure OL 8 to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.

Edit/modify the following line in the "/etc/pam.d/system-auth" file to include the sha512 option for pam_unix.so:

```
password sufficient pam_unix.so sha512
```


Internal Only - General

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

Internal Only - General

1.24 OL08-00-010160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "pam_unix.so" module must be configured in the password-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.

```
GROUP ID: V-248544
RULE ID: SV-248544r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

OL 8 systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify that the "pam_unix.so" module is configured to use sha512 in "/etc/pam.d/password-auth" with the following command:

```
$ sudo grep password /etc/pam.d/password-auth | grep pam_unix

password sufficient pam_unix.so sha512
```

If "sha512" is missing, or is commented out, this is a finding.

Remediation:

Configure OL 8 to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.

Edit/modify the following line in the "/etc/pam.d/password-auth" file to include the sha512 option for pam_unix.so:

```
password sufficient pam_unix.so sha512
```


Internal Only - General

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

Internal Only - General

1.25 OL08-00-010161 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent system daemons from using Kerberos for authentication.

```
GROUP ID: V-248545
RULE ID: SV-248545r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

OL 8 systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

The key derivation function (KDF) in Kerberos is not FIPS compatible. Ensuring the system does not have any keytab files present prevents system daemons from using Kerberos for authentication. A keytab is a file containing pairs of Kerberos principals and encrypted keys.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify that OL 8 prevents system daemons from using Kerberos for authentication.

If the system is a server using krb5-server-1.17-18.el8.x86_64 or newer, this requirement is not applicable.

If the system is a workstation using krb5-workstation-1.17-18.el8.x86_64 or newer, this requirement is not applicable.

Check if there are available keytabs with the following command:

```
$ sudo ls -al /etc/*.keytab
```

If this command produces any file(s), this is a finding.

Remediation:

Configure OL 8 to prevent system daemons from using Kerberos for authentication.

Remove any files with the `.keytab` extension from the operating system.

Internal Only - General

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

Internal Only - General

1.26 OL08-00-010162 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The krb5-workstation package must not be installed on OL 8.

```
GROUP ID: V-248546
RULE ID: SV-248546r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

OL 8 systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Currently, Kerberos does not use FIPS 140-2 cryptography.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify the krb5-workstation package has not been installed on the system with the following commands:

If the system is a server or is using krb5-workstation-1.17-18.el8.x86_64 or newer, this is Not Applicable.

```
$ sudo yum list installed krb5-workstation

krb5-workstation.x86_64 1.17-9.el8 repository
```

If the krb5-workstation package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the krb5-workstation package with the ISSO as an operational requirement or remove it from the system with the following command:

```
$ sudo yum remove krb5-workstation
```


Internal Only - General

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

Internal Only - General

1.27 OL08-00-010163 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The krb5-server package must not be installed on OL 8.

```
GROUP ID: V-248547
RULE ID: SV-248547r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

OL 8 systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Currently, Kerberos does not use FIPS 140-2 cryptography.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify the krb5-server package has not been installed on the system with the following commands:

If the system is a workstation or is using krb5-server-1.17-18.el8.x86_64 or newer, this is Not Applicable

```
$ sudo yum list installed krb5-server

krb5-server.x86_64 1.17-9.el8 repository
```

If the krb5-server package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the krb5-server package with the ISSO as an operational requirement or remove it from the system with the following command:

```
$ sudo yum remove krb5-server
```


Internal Only - General

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

Internal Only - General

1.28 OL08-00-010170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must use a Linux Security Module configured to enforce limits on system services.

```
GROUP ID: V-248548
RULE ID: SV-248548r958518
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security functionality includes but is not limited to establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is in "Enforcing" mode with the following command:

```
$ getenforce

Enforcing
```

If "SELinux" is not in "Enforcing" mode, this is a finding.

Remediation:

Configure OL 8 to verify correct operation of all security functions.

Set "SELinux" to "Enforcing" mode by modifying the "/etc/selinux/config" file with the following line:

```
SELINUX=enforcing
```

A reboot is required for the changes to take effect.

Internal Only - General

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

Internal Only - General

1.29 OL08-00-010171 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must have the "policycoreutils" package installed.

```
GROUP ID: V-248549
RULE ID: SV-248549r958518
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes but is not limited to establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Audit:

Verify the operating system has the "policycoreutils" package installed with the following command:

```
$ sudo yum list installed policycoreutils

policycoreutils.x86_64 2.9-3.el8 @anaconda
```

If the "policycoreutils" package is not installed, this is a finding.

Remediation:

Install the "policycoreutil" package, if it is not already installed, by running the following command:

```
$ sudo yum install policycoreutils
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

Internal Only - General

1.30 OL08-00-010190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A sticky bit must be set on all OL 8 public directories to prevent unauthorized and unintended information transferred via shared system resources.

```
GROUP ID: V-248551
RULE ID: SV-248551r958524
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Audit:

Verify that all world-writable directories have the sticky bit set.

Verify that all world-writable directories have the sticky bit set by running the following command:

```
$ sudo find / -type d \( -perm -0002 -a ! -perm -1000 \) -print 2>/dev/null
```

If any of the returned directories are world-writable and do not have the sticky bit set, this is a finding.

Internal Only - General

Remediation:

Configure all world-writable directories to have the sticky bit set to prevent unauthorized and unintended information transferred via shared system resources.

Set the sticky bit on all world-writable directories using the command, replace "[World-Writable Directory]" with any directory path missing the sticky bit:

```
$ sudo chmod 1777 [World-Writable Directory]
```

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

Internal Only - General

1.31 OL08-00-010200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.

```
GROUP ID: V-248552
RULE ID: SV-248552r986329
```

Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

OL 8 uses "/etc/ssh/sshd_config" for configurations of OpenSSH. Within the "sshd_config", the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" is used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the sshd_config man pages.

Satisfies: SRG-OS-000126-GPOS-00066, SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Internal Only - General

Audit:

Verify the SSH server automatically terminates a user session after the SSH client has become unresponsive.

Check that the "ClientAliveCountMax" is set to "1" by running the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*clientalivecountmax'

ClientAliveCountMax 1
```

If "ClientAliveCountMax" does not exist, does not have a product value of "1" in "/etc/ssh/sshd_config", or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Note: This setting must be applied in conjunction with OL08-00-010201 to function correctly.

Configure the SSH server to terminate a user session automatically after the SSH client has become unresponsive.

Modify or append the following line in the "/etc/ssh/sshd_config" file:

```
ClientAliveCountMax 1
```

For the changes to take effect, the SSH daemon must be restarted.

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

Internal Only - General

1.32 OL08-00-010201 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured so that all network connections associated with SSH traffic are terminated after 10 minutes of becoming unresponsive.

```
GROUP ID: V-248553
RULE ID: SV-248553r986330
```

Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

OL 8 uses "/etc/ssh/sshd_config" for configurations of OpenSSH. Within the "sshd_config", the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" is used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the sshd_config man pages.

Satisfies: SRG-OS-000126-GPOS-00066, SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Internal Only - General

Audit:

Verify the SSH server automatically terminates a user session after the SSH client has been unresponsive for 10 minutes.

Check that the "ClientAliveInterval" variable is set to a value of "600" or less by running the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*clientaliveinterval'

ClientAliveInterval 600
```

If "ClientAliveInterval" does not exist, does not have a product value of "600" or less in "/etc/ssh/sshd_config", or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Note: This setting must be applied in conjunction with OL08-00-010200 to function correctly.

Configure the SSH server to terminate a user session automatically after the SSH client has been unresponsive for 10 minutes.

Modify or append the following lines in the "/etc/ssh/sshd_config" file to have a product value of "600" or less:

```
ClientAliveInterval 600
```

The SSH daemon must be restarted for changes to take effect.

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

Internal Only - General

1.33 OL08-00-010210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "/var/log/messages" file must have mode 0640 or less permissive.

```
GROUP ID: V-248554
RULE ID: SV-248554r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the OL 8 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "/var/log/messages" file has mode "0640" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /var/log/messages

640 /var/log/messages
```

If a value of "0640" or less permissive is not returned, this is a finding.

Remediation:

Change the permissions of the file "/var/log/messages" to "0640" by running the following command:

```
$ sudo chmod 0640 /var/log/messages
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.34 OL08-00-010220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "/var/log/messages" file must be owned by root.

```
GROUP ID: V-248555
RULE ID: SV-248555r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the OL 8 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the /var/log/messages file is owned by root with the following command:

```
$ sudo stat -c "%U" /var/log/messages

root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the owner of the file /var/log/messages to root by running the following command:

```
$ sudo chown root /var/log/messages
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.35 OL08-00-010230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "/var/log/messages" file must be group-owned by root.

```
GROUP ID: V-248556
RULE ID: SV-248556r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the OL 8 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log/messages" file is group-owned by root with the following command:

```
$ sudo stat -c "%G" /var/log/messages

root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the group of the file "/var/log/messages" to "root" by running the following command:

```
$ sudo chgrp root /var/log/messages
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.36 OL08-00-010240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "/var/log" directory must have mode 0755 or less permissive.

```
GROUP ID: V-248557
RULE ID: SV-248557r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the OL 8 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "/var/log" directory has a mode of "0755" or less with the following command:

```
$ sudo stat -c "%a %n" /var/log

755 /var/log
```

If a value of "0755" or less permissive is not returned, this is a finding.

Remediation:

Change the permissions of the directory "/var/log" to "0755" by running the following command:

```
$ sudo chmod 0755 /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.37 OL08-00-010250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "/var/log" directory must be owned by root.

```
GROUP ID: V-248558
RULE ID: SV-248558r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the OL 8 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the /var/log directory is owned by root with the following command:

```
$ sudo stat -c "%U" /var/log

root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the owner of the directory /var/log to root by running the following command:

```
$ sudo chown root /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.38 OL08-00-010260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "/var/log" directory must be group-owned by root.

```
GROUP ID: V-248559
RULE ID: SV-248559r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the OL 8 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log" directory is group-owned by root with the following command:

```
$ sudo stat -c "%G" /var/log

root
```

If "root" is not returned as a result, this is a finding.

Remediation:

Change the group of the directory "/var/log" to "root" by running the following command:

```
$ sudo chgrp root /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.39 OL08-00-010287 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH daemon must be configured to use system-wide crypto policies.

```
GROUP ID: V-248560
RULE ID: SV-248560r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

OL 8 incorporates system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/ directory.

Audit:

Verify that system-wide crypto policies are in effect:

```
$ sudo grep -i CRYPTO_POLICY /etc/sysconfig/sshd

# CRYPTO_POLICY=
```

If the "CRYPTO_POLICY" is uncommented, this is a finding.

Remediation:

Configure the OL 8 SSH daemon to use system-wide crypto policies by adding the following line to /etc/sysconfig/sshd:

```
# CRYPTO_POLICY=
```

A reboot is required for the changes to take effect.

Internal Only - General

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Internal Only - General

1.40 OL08-00-010290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH server must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-2 validated cryptographic hash algorithms.

```
GROUP ID: V-248561
RULE ID: SV-248561r958510
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

OL 8 incorporates system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the "/etc/sysconfig/sshd" file. The employed algorithms can be viewed in the "/etc/crypto-policies/back-ends/opensshserver.config" file.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Audit:

Verify the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms with the following command:

```
 $ sudo grep -i macs /etc/crypto-policies/back-ends/opensshserver.config

 -oMACS=hmac-sha2-512,hmac-sha2-256,hmac-sha2-512-etm@openssh.com,hmac-sha2-
256-etm@openssh.com
```

If the MACs entries in the "opensshserver.config" file have any hashes other than shown here, the order differs from the example above, or they are missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure the OL 8 SSH server to use only MACs employing FIPS 140-2 approved algorithms:

Update the "/etc/crypto-policies/back-ends/opensshserver.config" file to include these MACs employing FIPS 140-2 approved algorithms:

```
-oMACS=hmac-sha2-512,hmac-sha2-256,hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

Internal Only - General

1.41 OL08-00-010291 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH server must be configured to use only ciphers employing FIPS 140-2 validated cryptographic algorithms.

```
GROUP ID: V-248562
RULE ID: SV-248562r958510
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest cipher available to secure the SSH connection.

Audit:

Verify the OL 8 SSH server is configured to use only ciphers employing FIPS 140-2 approved algorithms with the following command:

```
 $ sudo grep -i ciphers /etc/crypto-policies/back-ends/opensshserver.config

 CRYPTO_POLICY='-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr,aes256-
gcm@openssh.com,aes128-gcm@openssh.com'
```

If the cipher entries in the "opensshserver.config" file have any ciphers other than shown here, the order differs from the example above, or they are missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure the OL 8 SSH server to use only ciphers employing FIPS 140-2 approved algorithms:

Update the "/etc/crypto-policies/back-ends/opensshserver.config" file to include these ciphers employing FIPS 140-2-approved algorithms:

```
CRYPTO_POLICY='-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr,aes256-
gcm@openssh.com,aes128-gcm@openssh.com'
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

Internal Only - General

1.42 OL08-00-010292 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The OL 8 SSH server must be configured to use strong entropy.

```
GROUP ID: V-248563
RULE ID: SV-248563r991593
```

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The SSH implementation in OL 8 uses the OPENSSL library, which does not use high-entropy sources by default. By using the SSH_USE_STRONG_RNG environment variable, the OPENSSL random generator is reseeded from "/dev/random". This setting is not recommended on computers without the hardware random generator because insufficient entropy causes the connection to be blocked until enough entropy is available.

Audit:

Verify the operating system SSH server uses strong entropy with the following command:

```
$ sudo grep -i ssh_use_strong_rng /etc/sysconfig/sshd

SSH_USE_STRONG_RNG=32
```

If the "SSH_USE_STRONG_RNG" line does not equal "32" or is commented out or missing, this is a finding.

Remediation:

Configure the operating system SSH server to use strong entropy.

Add or modify the following line in the "/etc/sysconfig/sshd" file.

```
SSH_USE_STRONG_RNG=32
```

The SSH service must be restarted for changes to take effect.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.43 OL08-00-010293 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 operating system must implement DoD-approved encryption in the OpenSSL package.

```
GROUP ID: V-248564
RULE ID: SV-248564r1069146
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

OL 8 incorporates systemwide crypto policies by default. The employed algorithms can be viewed in the "/etc/crypto-policies/back-ends/openssl.config" file.

Audit:

Verify the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms:

Verify that systemwide crypto policies are in effect:

```
$ sudo grep -i opensslcnf.config /etc/pki/tls/openssl.cnf

.include /etc/crypto-policies/back-ends/opensslcnf.config
```

If the "opensslcnf.config" is not defined in the "/etc/pki/tls/openssl.cnf" file, this is a finding.

Verify which systemwide crypto policy is in use:

```
$ sudo fips-mode-setup --check

FIPS mode is enabled.
```

If the systemwide crypto policy is set to anything other than "FIPS", this is a finding.

Internal Only - General

Remediation:

Configure the OL 8 OpenSSL library to use only ciphers employing FIPS 140-2 approved algorithms with the following command:

```
$ sudo fips-mode-setup --enable
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Internal Only - General

1.44 OL08-00-010294 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 operating system must implement DoD-approved TLS encryption in the OpenSSL package.

```
GROUP ID: V-248565
RULE ID: SV-248565r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

OL 8 incorporates system-wide crypto policies by default. The employed algorithms can be viewed in the "/etc/crypto-policies/back-ends/openssl.config" file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

Internal Only - General

Audit:

Verify the OpenSSL library is configured to use only DoD-approved TLS encryption:

For versions prior to crypto-policies-20210617-1.gitc776d3e.el8.noarch:

```
$ sudo grep -i MinProtocol /etc/crypto-policies/back-ends/opensslcnf.config

MinProtocol = TLSv1.2
```

If the "MinProtocol" is set to anything older than "TLSv1.2", this is a finding.

For version crypto-policies-20210617-1.gitc776d3e.el8.noarch and newer:

```
$ sudo grep -i  MinProtocol /etc/crypto-policies/back-ends/opensslcnf.config

TLS.MinProtocol = TLSv1.2
DTLS.MinProtocol = DTLSv1.2
```

If the "TLS.MinProtocol" is set to anything older than "TLSv1.2" or the "DTLS.MinProtocol" is set to anything older than "DTLSv1.2", this is a finding.

Remediation:

Configure the OL 8 OpenSSL library to use only DoD-approved TLS encryption by editing the following line in the "/etc/crypto-policies/back-ends/opensslcnf.config" file:

For versions prior to crypto-policies-20210617-1.gitc776d3e.el8.noarch:

```
MinProtocol = TLSv1.2
```

For version crypto-policies-20210617-1.gitc776d3e.el8.noarch and newer:

- TLS.MinProtocol = TLSv1.2
- DTLS.MinProtocol = DTLSv1.2

A reboot is required for the changes to take effect.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Internal Only - General

1.45 OL08-00-010295 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 operating system must implement DoD-approved TLS encryption in the GnuTLS package.

```
GROUP ID: V-248566
RULE ID: SV-248566r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Transport Layer Security (TLS) encryption is a required security setting as a number of known vulnerabilities have been reported against Secure Sockets Layer (SSL) and earlier versions of TLS. Encryption of private information is essential to ensuring data confidentiality. If private information is not encrypted, it can be intercepted and easily read by an unauthorized party. SQL Server must use a minimum of FIPS 140-2 approved TLS version 1.2, and all non-FIPS-approved SSL and TLS versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

The GnuTLS library offers an API to access secure communications protocols. SSLv2 is not available in the GnuTLS library. The OL 8 system-wide crypto policy defines employed algorithms in the "/etc/crypto-policies/back-ends/gnutls.config" file.

Audit:

Verify the GnuTLS library is configured to only allow DoD-approved SSL/TLS versions:

```
$ sudo grep -io +vers.* /etc/crypto-policies/back-ends/gnutls.config

+VERS-ALL:-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-
DTLS1.0:+COMP-NULL:%PROFILE_MEDIUM
```

If the "gnutls.config" does not list "-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-DTLS1.0" to disable unapproved SSL/TLS versions, this is a finding.

Internal Only - General

Remediation:

Configure the OL 8 GnuTLS library to use only DoD-approved encryption by adding the following line to "/etc/crypto-policies/back-ends/gnutls.config":

```
+VERS-ALL:-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-DTLS1.0
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Internal Only - General

1.46 OL08-00-010300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 system commands must have mode 755 or less permissive.

```
GROUP ID: V-248567
RULE ID: SV-248567r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories have mode "755" or less permissive with the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -
perm /022 -exec ls -l {} \;
```

If any system commands are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command with a mode more permissive than "755".

```
$ sudo chmod 755 [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.47 OL08-00-010310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 system commands must be owned by root.

```
GROUP ID: V-248568
RULE ID: SV-248568r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are owned by "root" with the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin !
-user root -exec ls -l {} \;
```

If any system commands are returned, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command file not owned by "root".

```
$ sudo chown root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.48 OL08-00-010320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 system commands must be group-owned by root or a system account.

```
GROUP ID: V-248569
RULE ID: SV-248569r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are group-owned by "root" or a required system account, with the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin !
-group root -exec ls -l {} \;
```

If any system commands are returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command file not group-owned by "root" or a required system account.

```
$ sudo chgrp root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.49 OL08-00-010330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 library files must have mode 755 or less permissive.

```
GROUP ID: V-248570
RULE ID: SV-248570r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files contained in the following directories have mode "755" or less permissive with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type f -exec ls -l
{} \;
```

If any system-wide shared library file is found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the library files to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any library file with a mode more permissive than 755.

```
$ sudo chmod 755 [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.50 OL08-00-010331 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 library directories must have mode 755 or less permissive.

```
GROUP ID: V-252651
RULE ID: SV-252651r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library directories within "/lib", "/lib64", "/usr/lib" and "/usr/lib64" have mode "755" or less permissive with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type d -exec stat -c
"%n %a" '{}' \;
```

If any system-wide shared library directories are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the library directories to be protected from unauthorized access. Run the following command, replacing "[DIRECTORY]" with any library directory with a mode more permissive than 755.

```
$ sudo chmod 755 [DIRECTORY]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.51 OL08-00-010340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 library files must be owned by root.

```
GROUP ID: V-248571
RULE ID: SV-248571r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files are owned by "root" with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 ! -user root -exec ls -l {} \;
```

If any system-wide shared library file is returned, this is a finding.

Remediation:

Configure the system-wide shared library files (/lib, /lib64, /usr/lib, and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any library file not owned by "root".

```
$ sudo chown root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.52 OL08-00-010341 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 library directories must be owned by root.

```
GROUP ID: V-252652
RULE ID: SV-252652r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library directories are owned by "root" with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type d -exec stat -
c "%n %U" '{}' \;
```

If any system wide shared library directory is returned, this is a finding.

Remediation:

Configure the system-wide shared library directories within (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[DIRECTORY]" with any library directory not owned by "root".

```
$ sudo chown root [DIRECTORY]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.53 OL08-00-010350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 library files must be group-owned by root.

```
GROUP ID: V-248572
RULE ID: SV-248572r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files are group-owned by "root" with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 ! -group root -exec ls -l {}
\;
```

If any system-wide shared library file is returned, this is a finding.

Remediation:

Configure the system-wide shared library files (/lib, /lib64, /usr/lib, and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any library file not group-owned by "root".

```
$ sudo chgrp root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.54 OL08-00-010351 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 library directories must be group-owned by root or a system account.

```
GROUP ID: V-252653
RULE ID: SV-252653r991560
```

Rationale:

If OL 8 were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to OL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library directories are group-owned by "root" with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type d -exec stat
-c "%n %G" '{}' \;
```

If any system wide shared library directory is returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure the system-wide shared library directories (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[DIRECTORY]" with any library directory not group-owned by "root".

```
$ sudo chgrp root [DIRECTORY]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

Internal Only - General

1.55 OL08-00-010358 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured to allow sending email notifications of unauthorized configuration changes to designated personnel.

```
GROUP ID: V-256979
RULE ID: SV-256979r958794
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Audit:

Verify that the operating system is configured to allow sending email notifications.

Note: The "mailx" package provides the "mail" command that is used to send email messages.

Verify that the "mailx" package is installed on the system:

```
 $ sudo yum list installed mailx

 mailx.x86_64     12.5-29.el8     @ol8_baseos_latest
```

If "mailx" package is not installed, this is a finding.

Remediation:

Install the "mailx" package on the system:

```
 $ sudo yum install mailx
```

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 5::CM-3 (5)
- NIST SP 800-53 Revision 4::CM-3 (5)

Internal Only - General

1.56 OL08-00-010359 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 operating system must use a file integrity tool to verify correct operation of all security functions.

```
GROUP ID: V-252654
RULE ID: SV-252654r958944
```

Rationale:

Without verification of the security functions, security functions may not operate correctly, and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to the OL 8 operating system performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is installed and verifies the correct operation of all security functions.

Check that the AIDE package is installed with the following command:

$ sudo rpm -q aide

```
 aide-0.16-14.el8_5.1.x86_64
```

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

If there is no application installed to perform integrity checks, this is a finding.

If AIDE is installed, check if it has been initialized with the following command:

$ sudo /usr/sbin/aide --check

If the output is "Couldn't open file /var/lib/aide/aide.db.gz for reading", this is a finding.

Internal Only - General

Remediation:

Install AIDE, initialize it, and perform a manual check.

Install AIDE:

```
$ sudo yum install aide
```

Initialize it:

```
$ sudo /usr/sbin/aide --init
```

Example output:

Number of entries: 48623

```
---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db.new.gz
  SHA1     : LTAVQ8tFJthsrf4m9gfRpnf1vyc=
  SHA256   : NJ9+uzRQKSwmLQ8A6IpKNvYjVKGbhSjt
             BeJBVcmOVrI=
  SHA512   : 7d8I/F6A1b07E4ZuGeilZjefRgJJ/F20
             eC2xoag1OsOVpctt3Mi7Jjjf3vFW4xoY
             5mdS6/ImQpm0xtlTLOPeQQ==

End timestamp: 2022-10-20 10:50:52 -0700 (run time: 0m 46s)
```

The new database will need to be renamed to be read by AIDE:

```
$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Perform a manual check:

```
$ sudo /usr/sbin/aide --check
```

Example output:

```
Start timestamp: 2022-10-20 11:03:16 -0700 (AIDE 0.16)
AIDE found differences between database and filesystem!!
...

Done.
```

Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4::SI-6 a
- NIST SP 800-53 Revision 5::SI-6 a

Internal Only - General

1.57 OL08-00-010360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 file integrity tool must notify the system administrator (SA) when changes to the baseline configuration or anomalies in the operation of any security functions are discovered within an organizationally defined frequency.

```
GROUP ID: V-248573
RULE ID: SV-248573r1069152
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's information system security manager (ISSM)/information system security officer (ISSO) and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Notifications provided by information systems include messages to local computer consoles and/or hardware indications, such as lights.

This capability must take into account operational requirements for availability for selecting an appropriate response. The organization may choose to shut down or restart the information system upon security function anomaly detection.

OL 8 comes with many optional software packages, including the file integrity tool Advanced Intrusion Detection Environment (AIDE). This requirement assumes the use of AIDE; however, a different tool may be used if the requirements are met. Note that AIDE does not have a configuration that will send a notification, so a cron job is recommended that uses the mail application on the system to email the results of the file integrity check.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000446-GPOS-00200, SRG-OS-000447-GPOS-00201

Internal Only - General

Audit:

Verify the operating system routinely checks the baseline configuration for unauthorized changes and notifies the SA when anomalies in the operation of any security functions are discovered.

Check that OL 8 routinely executes a file integrity scan for changes to the system baseline. The command used in the example will use a daily occurrence.

Check the cron directories for scripts controlling the execution and notification of results of the file integrity application. For example, if AIDE is installed on the system, use the following commands:

To search for an aide script:

```
$ sudo ls -al /etc/cron.* | grep aide

-rwxr-xr-x 1 root root 29 Nov 22 2015 aide
```

To search for scheduled cron jobs:

```
$ sudo grep -r aide /etc/cron*

/etc/cron.d/aide:0 0 * * * root /usr/sbin/aide --check | /bin/mail -s
"$HOSTNAME - Daily AIDE integrity check run" root@example_server_name.mil
```

Check the contents of script files:

```
$ sudo more /etc/cron.d/aide

#!/bin/bash
/usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily AIDE integrity check
run" root@example_server_name.mil
```

If the file integrity application does not exist, a script file controlling the execution of the file integrity application does not exist, or the file integrity application does not notify designated personnel of changes, this is a finding.

Internal Only - General

Remediation:

Configure the file integrity tool to run automatically on the system at least weekly and to notify designated personnel if baseline configurations are changed in an unauthorized manner. The AIDE tool can be configured to email designated personnel with the use of the cron system.

The following example output is generic. It will set cron to run AIDE daily and to send an email at the completion of the analysis. The file path in the more command is exemplary. Common paths include /etc/cron.d/, /etc/cron.daily/, /etc/cron.hourly/, /etc/cron.weekly/, or /etc/cron.monthly/.

```
$ sudo more /etc/cron.d/aide
#!/bin/bash

/usr/sbin/aide --check |/bin/mail -s "$HOSTNAME - Daily AIDE integrity check
run" root@example_server_name.mil
```

Note: Per requirement OL08-00-010358, the "mailx" package must be installed on the system to enable email functionality.

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 5::CM-3 (5)
- NIST SP 800-53 Revision 4::CM-3 (5)

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4::SI-6 b
- NIST SP 800-53 Revision 5::SI-6 b

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4::SI-6 d
- NIST SP 800-53 Revision 5::SI-6 d

Internal Only - General

1.58 OL08-00-010370 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

YUM must be configured to prevent the installation of patches, service packs, device drivers, or OL 8 system components that have not been digitally signed using a certificate that is recognized and approved by the organization.

```
GROUP ID: V-248574
RULE ID: SV-248574r1015031
```

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DOD certificates for this purpose; however, the certificate used to verify the software must be from an approved Certificate Authority (CA).

Audit:

Check that YUM verifies the signature of packages from a repository prior to install with the following command:

```
$ sudo grep gpgcheck /etc/yum.repos.d/*.repo

gpgcheck=1
```

If "gpgcheck" is not set to "1", or if options are missing or commented out, ask the system administrator (SA) how the certificates for patches and other operating system components are verified.

If there is no process to validate certificates that is approved by the organization, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to verify the signature of packages from a repository prior to install by setting the following option in the "/etc/yum.repos.d/[your_repo_name].repo" file:

```
gpgcheck=1
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

Internal Only - General

1.59 OL08-00-010371 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

```
GROUP ID: V-248575
RULE ID: SV-248575r1015032
```

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DOD certificates for this purpose; however, the certificate used to verify the software must be from an approved Certificate Authority (CA).

Audit:

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components from a repository without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check if YUM is configured to perform a signature check on local packages with the following command:

```
$ sudo grep -i localpkg_gpgcheck /etc/dnf/dnf.conf

localpkg_gpgcheck =True
```

If "localpkg_gpgcheck" is not set to either "1", "True", or "yes", commented out, or is missing from "/etc/dnf/dnf.conf", this is a finding.

Internal Only - General

Remediation:

Configure the operating system to remove all software components after updated versions have been installed.

Set the "localpkg_gpgcheck" option to "True" in the "/etc/dnf/dnf.conf" file:

```
localpkg_gpgcheck=True
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

Internal Only - General

1.60 OL08-00-010372 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent the loading of a new kernel for later execution.

```
GROUP ID: V-248576
RULE ID: SV-248576r1015033
```

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Disabling "kexec_load" prevents an unsigned kernel image (that could be a windows kernel or modified vulnerable kernel) from being loaded. Kexec can be used to subvert the entire secureboot process and should be avoided at all costs, especially since it can load unsigned kernel images.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Note: For OL 8 systems using the Oracle Unbreakable Enterprise Kernel (UEK) Release 6 or above and with secureboot enabled, this requirement is Not Applicable.

Verify the operating system is configured to disable kernel image loading with the following commands.

Check the status of the "kernel.kexec_load_disabled" kernel parameter:

```
$ sudo sysctl kernel.kexec_load_disabled

kernel.kexec_load_disabled = 1
```

If "kernel.kexec_load_disabled" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter:

```
$ sudo grep -r kernel.kexec_load_disabled /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:kernel.kexec_load_disabled = 1
```

If "kernel.kexec_load_disabled" is not set to "1" or is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to disable kernel image loading.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.kexec_load_disabled = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```


Internal Only - General

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

Internal Only - General

1.61 OL08-00-010373 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable kernel parameters to enforce Discretionary Access Control (DAC) on symlinks.

```
GROUP ID: V-248577
RULE ID: SV-248577r958702
```

Rationale:

DAC is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When DAC policies are implemented, subjects are not constrained as to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control (MAC) policies is still able to operate under the less rigorous constraints of this requirement. Therefore, while MAC imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of DAC require identity-based access control, that limitation is not required for this use of DAC.

By enabling the "fs.protected_symlinks" kernel parameter, symbolic links are permitted to be followed only when outside a sticky world-writable directory, or when the UID of the link and follower match, or when the directory owner matches the symlink's owner. Disallowing such symlinks helps mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Internal Only - General

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify the operating system is configured to enable DAC on symlinks with the following commands.

Check the status of the "fs.protected_symlinks" kernel parameter:

```
$ sudo sysctl fs.protected_symlinks

fs.protected_symlinks = 1
```

If "fs.protected_symlinks" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter:

```
$ sudo grep -r fs.protected_symlinks /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:fs.protected_symlinks = 1
```

If "fs.protected_symlinks" is not set to "1" or is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to enable DAC on symlinks.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
fs.protected_symlinks = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

Internal Only - General

1.62 OL08-00-010375 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must restrict access to the kernel message buffer.

```
GROUP ID: V-248579
RULE ID: SV-248579r958524
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Restricting access to the kernel message buffer limits access to only root. This prevents attackers from gaining additional system information as a non-privileged user.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify the operating system is configured to restrict access to the kernel message buffer with the following commands.

Check the status of the "kernel.dmesg_restrict" kernel parameter:

```
$ sudo sysctl kernel.dmesg_restrict

kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter:

```
$ sudo grep -r kernel.dmesg_restrict /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1" or is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to restrict access to the kernel message buffer.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.dmesg_restrict = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

Internal Only - General

1.63 OL08-00-010376 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must prevent kernel profiling by unprivileged users.

```
GROUP ID: V-248580
RULE ID: SV-248580r958524
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Setting the "kernel.perf_event_paranoid" kernel parameter to "2" prevents attackers from gaining additional system information as a non-privileged user.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify the operating system is configured to prevent kernel profiling by unprivileged users with the following commands.

Check the status of the "kernel.perf_event_paranoid" kernel parameter:

```
$ sudo sysctl kernel.perf_event_paranoid

kernel.perf_event_paranoid = 2
```

If "kernel.perf_event_paranoid" is not set to "2" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter:

```
$ sudo grep -r kernel.perf_event_paranoid /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:kernel.perf_event_paranoid = 2
```

If "kernel.perf_event_paranoid" is not set to "2" or is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to prevent kernel profiling by unprivileged users.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.perf_event_paranoid = 2
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

Internal Only - General

1.64 OL08-00-010374 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable kernel parameters to enforce Discretionary Access Control (DAC) on hardlinks.

```
GROUP ID: V-248578
RULE ID: SV-248578r958702
```

Rationale:

DAC is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When DAC policies are implemented, subjects are not constrained as to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control (MAC) policies is still able to operate under the less rigorous constraints of this requirement. Therefore, while MAC imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of DAC require identity-based access control, that limitation is not required for this use of DAC.

By enabling the "fs.protected_hardlinks" kernel parameter, users can no longer create soft or hard links to files they do not own. Disallowing such hardlinks mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Internal Only - General

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify the operating system is configured to enable DAC on hardlinks with the following commands.

Check the status of the "fs.protected_hardlinks" kernel parameter:

```
$ sudo sysctl fs.protected_hardlinks

fs.protected_hardlinks = 1
```

If "fs.protected_hardlinks" is not set to "1" or is missing, this is a finding.

Check that the configuration files are present to enable this kernel parameter:

```
$ sudo grep -r fs.protected_hardlinks /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:fs.protected_hardlinks = 1
```

If "fs.protected_hardlinks" is not set to "1" or is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to enable DAC on hardlinks.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
fs.protected_hardlinks = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4::AC-3 (4)
- NIST SP 800-53 Revision 5::AC-3 (4)

Internal Only - General

1.65 OL08-00-010379 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must specify the default "include" directory for the /etc/sudoers file.

```
GROUP ID: V-252655
RULE ID: SV-252655r991589
```

Rationale:

The "sudo" command allows authorized users to run programs (including shells) as other users, system users, and root. The "/etc/sudoers" file is used to configure authorized "sudo" users as well as the programs they are allowed to run. Some configuration options in the "/etc/sudoers" file allow configured users to run programs without re-authenticating. Use of these configuration options makes it easier for one compromised account to be used to compromise other accounts.

It is possible to include other sudoers files from within the sudoers file currently being parsed using the #include and #includedir directives. When sudo reaches this line it will suspend processing of the current file (/etc/sudoers) and switch to the specified file/directory. Once the end of the included file(s) are reached, the rest of /etc/sudoers will be processed. Files that are included may themselves include other files. A hard limit of 128 nested include files is enforced to prevent include file loops.

Audit:

Note: If the "include" and "includedir" directives are not present in the /etc/sudoers file, this requirement is not applicable.

Verify the operating system specifies only the default "include" directory for the /etc/sudoers file with the following command:

```
 $ sudo grep include /etc/sudoers

 #includedir /etc/sudoers.d
```

If the results are not "/etc/sudoers.d" or additional files or directories are specified, this is a finding.

Verify the operating system does not have nested "include" files or directories within the /etc/sudoers.d directory with the following command:

```
 $ sudo grep -Er include /etc/sudoers.d
```

If results are returned, this is a finding.

Internal Only - General

Remediation:

Configure the /etc/sudoers file to only include the /etc/sudoers.d directory.

Edit the /etc/sudoers file with the following command:

```
$ sudo visudo
```

Add or modify the following line:

#includedir /etc/sudoers.d

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.66 OL08-00-010380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must require users to provide a password for privilege escalation.

```
GROUP ID: V-248581
RULE ID: SV-248581r1050789
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify that "/etc/sudoers" has no occurrences of "NOPASSWD".

Check that the "/etc/sudoers" file has no occurrences of "NOPASSWD" by running the following command:

```
$ sudo grep -ir nopasswd /etc/sudoers /etc/sudoers.d

%admin ALL=(ALL) NOPASSWD: ALL
```

If any occurrences of "NOPASSWD" are returned from the command and have not been documented with the information system security officer (ISSO) as an organizationally defined administrative group using multifactor authentication (MFA), this is a finding.

Internal Only - General

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the "/etc/sudoers" file with the following command:

```
$ sudo visudo
```

Remove any occurrences of "NOPASSWD" tags in the file.

Check the configuration of the /etc/sudoers.d/* files with the following command:

```
$ sudo grep -ir nopasswd /etc/sudoers.d
```

Remove any occurrences of "NOPASSWD" tags in the file.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

Internal Only - General

1.67 OL08-00-010381 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must require users to reauthenticate for privilege escalation and changing roles.

```
GROUP ID: V-248582
RULE ID: SV-248582r1050789
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify that the "/etc/sudoers" file has no occurrences of "!authenticate" by running the following command:

```
 $ sudo grep -Ei !authenticate /etc/sudoers /etc/sudoers.d/*
```

If any occurrences of "!authenticate" return from the command, this is a finding.

Remediation:

Remove any occurrence of "!authenticate" found in the "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

Internal Only - General

1.68 OL08-00-010382 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must restrict privilege elevation to authorized personnel.

```
GROUP ID: V-248583
RULE ID: SV-248583r991589
```

Rationale:

The sudo command allows a user to execute programs with elevated (administrator) privileges. It prompts the user for their password and confirms your request to execute a command by checking a file, called sudoers. If the "sudoers" file is not configured correctly, any user defined on the system can initiate privileged actions on the target system.

Audit:

Verify the "sudoers" file restricts sudo access to authorized personnel.

```
$ sudo grep -iw 'ALL' /etc/sudoers /etc/sudoers.d/*
```

If the either of the following entries are returned, this is a finding:

```
ALL     ALL=(ALL) ALL
ALL     ALL=(ALL:ALL) ALL
```

Remediation:

Remove the following entries from the sudoers file:

```
ALL     ALL=(ALL) ALL
ALL     ALL=(ALL:ALL) ALL
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.69 OL08-00-010383 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must use the invoking user's password for privilege escalation when using "sudo".

```
GROUP ID: V-248584
RULE ID: SV-248584r991589
```

Rationale:

The sudoers security policy requires that users authenticate themselves before they can use sudo. When sudoers requires authentication, it validates the invoking user's credentials. If the rootpw, targetpw, or runaspw flags are defined and not disabled, by default the operating system will prompt the invoking user for the "root" user password. For more information on each of the listed configurations, reference the sudoers(5) manual page.

Audit:

Verify that the sudoers security policy is configured to use the invoking user's password for privilege escalation.

```
 $ sudo grep -Eir '(rootpw|targetpw|runaspw)' /etc/sudoers /etc/sudoers.d* |
grep -v '#'

 /etc/sudoers:Defaults !targetpw
 /etc/sudoers:Defaults !rootpw
 /etc/sudoers:Defaults !runaspw
```

If conflicting results are returned, this is a finding.

If "Defaults !targetpw" is not defined, this is a finding.

If "Defaults !rootpw" is not defined, this is a finding.

If "Defaults !runaspw" is not defined, this is a finding.

Internal Only - General

Remediation:

Define the following in the Defaults section of the /etc/sudoers file or a configuration file in the /etc/sudoers.d/ directory:

```
Defaults !targetpw
Defaults !rootpw
Defaults !runaspw
```

Remove any configurations that conflict with the above from the following locations:

```
/etc/sudoers
/etc/sudoers.d/
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.70 OL08-00-010384 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must require reauthentication when using the "sudo" command.

```
GROUP ID: V-248585
RULE ID: SV-248585r1050789
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the organization requires the user to reauthenticate when using the "sudo" command.

If the value is set to an integer less than 0, the user's time stamp will not expire and the user will not have to reauthenticate for privileged actions until the user's session is terminated.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify the operating system requires re-authentication when using the "sudo" command to elevate privileges.

```
 $ sudo grep -Eir 'timestamp_timeout' /etc/sudoers /etc/sudoers.d*
 /etc/sudoers:Defaults timestamp_timeout=0
```

If conflicting results are returned, this is a finding.

If "timestamp_timeout" is set to a negative number, is commented out, or no results are returned, this is a finding.

Internal Only - General

Remediation:

Configure the "sudo" command to require re-authentication.

Edit the /etc/sudoers file:

```
$ sudo visudo
```

Add or modify the following line:

```
Defaults timestamp_timeout=[value]
```

Note: The "[value]" must be a number that is greater than or equal to "0".

Remove any duplicate or conflicting lines from /etc/sudoers and /etc/sudoers.d/ files.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

Internal Only - General

1.71 OL08-00-010385 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 operating system must not be configured to bypass password requirements for privilege escalation.

```
GROUP ID: V-252656
RULE ID: SV-252656r1050789
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify the operating system is not be configured to bypass password requirements for privilege escalation.

Check the configuration of the "/etc/pam.d/sudo" file with the following command:

```
$ sudo grep pam_succeed_if /etc/pam.d/sudo
```

If any occurrences of "pam_succeed_if" is returned from the command, this is a finding.

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the "/etc/ pam.d/sudo" file with the following command:

```
$ sudo vi /etc/pam.d/sudo
```

Remove any occurrences of " pam_succeed_if " in the file.

Internal Only - General

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

Internal Only - General

1.72 OL08-00-010390 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must have the package required for multifactor authentication installed.

```
GROUP ID: V-248586
RULE ID: SV-248586r1015037
```

Rationale:

Using an authentication device, such as a DOD Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DOD CAC.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Audit:

Verify the operating system has the package required for multifactor authentication installed with the following command:

```
$ sudo yum list installed openssl-pkcs11

openssl-pkcs11.x86_64 0.4.8-2.el8 @anaconda
```

If the "openssl-pkcs11" package is not installed, ask the administrator to indicate what type of multifactor authentication is being used and what packages are installed to support it.

If there is no evidence of multifactor authentication being used, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to implement multifactor authentication by installing the required package with the following command:

```
$ sudo yum install  openssl-pkcs11
```

Additional Information:

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 4::IA-2 (11)

Internal Only - General

1.73 OL08-00-010400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must implement certificate status checking for multifactor authentication.

```
GROUP ID: V-248587
RULE ID: SV-248587r1015038
```

Rationale:

Using an authentication device, such as a DOD Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DOD CAC.

OL 8 includes multiple options for configuring certificate status checking but for this requirement focuses on the system security services daemon (sssd). By default, sssd performs Online Certificate Status Protocol (OCSP) checking and certificate verification using a sha256 digest function.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000377-GPOS-00162

Audit:

Verify the operating system implements certificate status checking for multifactor authentication.

Note: If the system administrator (SA) demonstrates the use of an approved alternate multifactor authentication method, this requirement is not applicable.

Determine if Online Certificate Status Protocol (OCSP) is enabled and using the proper digest value on the system with the following command:

```
$ sudo grep certificate_verification /etc/sssd/sssd.conf
/etc/sssd/conf.d/*.conf | grep -v "^#"

certificate_verification = ocsp_dgst=sha1
```

If the certificate_verification line is missing from the [sssd] section, or is missing "ocsp_dgst=sha1", ask the administrator to indicate what type of multifactor authentication is being used and how the system implements certificate status checking. If there is no evidence of certificate status checking being used, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to implement certificate status checking for multifactor authentication.

Review the "/etc/sssd/sssd.conf" file to determine if the system is configured to prevent OCSP or certificate verification.

Add the following line to the [sssd] section of the "/etc/sssd/sssd.conf" file:

```
certificate_verification = ocsp_dgst=sha1
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```

Additional Information:

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 4::IA-2 (11)

Internal Only - General

1.74 OL08-00-010410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must accept Personal Identity Verification (PIV) credentials.

```
GROUP ID: V-248588
RULE ID: SV-248588r958816
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

The DoD has mandated the use of the Common Access Card (CAC) to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

Audit:

Verify OL 8 accepts PIV credentials.

Check that the "opensc" package is installed on the system with the following command:

```
$ sudo yum list installed opensc

opensc.x86_64     0.19.0-5.el8     @anaconda
```

Check that "opensc" accepts PIV cards with the following command:

```
$ sudo opensc-tool --list-drivers | grep -i piv

PIV-II     Personal Identity Verification Card
```

If the "opensc" package is not installed and the "opensc-tool" driver list does not include "PIV-II", this is a finding.

Remediation:

Configure OL 8 to accept PIV credentials.

Install the "opensc" package using the following command:

```
$ sudo yum install opensc
```

Additional Information:

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

Internal Only - General

1.75 OL08-00-010420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must implement non-executable data to protect its memory from unauthorized code execution.

```
GROUP ID: V-248589
RULE ID: SV-248589r958928
```

Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

Audit:

Verify the NX (no-execution) bit flag is set on the system with the following commands:

```
$ sudo dmesg | grep NX

[ 0.000000] NX (Execute Disable) protection: active
```

If "dmesg" does not show "NX (Execute Disable) protection" active, check the "cpuinfo" settings with the following command:

```
$ sudo less /proc/cpuinfo | grep -i flags

flags : fpu vme de pse tsc ms nx rdtscp lm constant_tsc
```

If "flags" does not contain the "nx" flag, this is a finding.

Remediation:

Enable the NX bit execute protection in the system BIOS.

Additional Information:

CCI-002824 Implement organization-defined controls to protect the system memory from unauthorized code execution.

- NIST SP 800-53 Revision 4::SI-16
- NIST SP 800-53 Revision 5::SI-16

Internal Only - General

1.76 OL08-00-010421 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must clear the page allocator to prevent use-after-free attacks.

```
GROUP ID: V-248590
RULE ID: SV-248590r958518
```

Rationale:

Adversaries may launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

Audit:

Verify that GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities with the following commands:

```
$ sudo grub2-editenv list | grep page_poison

kernelopts=root=/dev/mapper/ol-root ro crashkernel=auto
resume=/dev/mapper/ol-swap rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb quiet
fips=1 page_poison=1 vsyscall=none audit=1 audit_backlog_limit=8192
boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "page_poison" is not set to "1" or is missing, this is a finding.

Check that page poisoning is enabled by default to persist in kernel updates:

```
$ sudo grep page_poison /etc/default/grub

GRUB_CMDLINE_LINUX="page_poison=1"
```

If "page_poison" is not set to "1" or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to enable page poisoning with the following commands:

```
$ sudo grubby --update-kernel=ALL --args="page_poison=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="page_poison=1"
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

Internal Only - General

1.77 OL08-00-010422 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable virtual syscalls.

```
GROUP ID: V-248591
RULE ID: SV-248591r958518
```

Rationale:

Syscalls are special routines in the Linux kernel, which userspace applications ask to do privileged tasks. Invoking a system call is an expensive operation because the processor must interrupt the currently executing task and switch context to kernel mode and then back to userspace after the system call completes. Virtual syscalls map into user space a page that contains some variables and the implementation of some system calls. This allows the system calls to be executed in userspace to alleviate the context switching expense.

Virtual syscalls provide an opportunity of attack for a user who has control of the return instruction pointer. Disabling vsyscalls help to prevent return-oriented programming (ROP) attacks via buffer overflows and overruns. If the system intends to run containers based on OL 6 components, then virtual syscalls will need enabled so the components function properly.

Audit:

Verify that GRUB 2 is configured to disable vsyscalls with the following commands:

```
$ sudo grub2-editenv list | grep vsyscall

kernelopts=root=/dev/mapper/ol-root ro crashkernel=auto
resume=/dev/mapper/ol-swap rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb quiet
fips=1 page_poison=1 vsyscall=none audit=1 audit_backlog_limit=8192
boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "vsyscall" is not set to "none" or is missing, this is a finding.

Check that vsyscalls are disabled by default to persist in kernel updates:

```
$ sudo grep vsyscall /etc/default/grub

GRUB_CMDLINE_LINUX="vsyscall=none"
```

If "vsyscall" is not set to "none", is missing or commented out and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Document the use of vsyscalls with the ISSO as an operational requirement or disable them with the following command:

```
$ sudo grubby --update-kernel=ALL --args="vsyscall=none"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="vsyscall=none"
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

Internal Only - General

1.78 OL08-00-010423 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must clear memory when it is freed to prevent use-after-free attacks.

```
GROUP ID: V-248592
RULE ID: SV-248592r1069149
```

Rationale:

Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

init_on_free is a Linux kernel boot parameter that enhances security by initializing memory regions when they are freed, preventing data leakage. This process ensures that stale data in freed memory cannot be accessed by malicious programs.

SLUB canaries add a randomized value (canary) at the end of SLUB-allocated objects to detect memory corruption caused by buffer overflows or underflows. Redzoning adds padding (red zones) around SLUB-allocated objects to detect overflows or underflows by triggering a fault when adjacent memory is accessed. SLUB canaries are often more efficient and provide stronger detection against buffer overflows compared to redzoning. SLUB canaries are supported in hardened Linux kernels like the ones provided by Linux-hardened.

SLAB objects are blocks of physically contiguous memory. SLUB is the unqueued SLAB allocator.

Satisfies: SRG-OS-000433-GPOS-00192, SRG-OS-000134-GPOS-00068

Internal Only - General

Audit:

Verify GRUB2 is configured to mitigate use-after-free vulnerabilities by employing memory poisoning.

Inspect the "GRUB_CMDLINE_LINUX" entry of /etc/default/grub as follows:

```
$ sudo grep -i grub_cmdline_linux /etc/default/grub

GRUB_CMDLINE_LINUX="... init_on_free=1"
```

If "init_on_free=1" is missing or commented out, this is a finding.

Remediation:

Configure OL 8 to enable init_on_free with the following command:

```
$ sudo grubby --update-kernel=ALL --args="init_on_free=1"
```

Regenerate the GRUB configuration:

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Reboot the system:

```
$ sudo reboot
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

Internal Only - General

1.79 OL08-00-010424 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not let Meltdown and Spectre exploit critical vulnerabilities in modern processors.

```
GROUP ID: V-248593
RULE ID: SV-248593r1069159
```

Rationale:

Hardware vulnerabilities allow programs to steal data that is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to obtain secrets stored in the memory of other running programs. This might include passwords stored in a password manager or browser; personal photos, emails, and instant messages; and business-critical documents.

Audit:

Verify OL 8 is configured to enable mitigations with the following command:

```
$ grubby --info=/boot/vmlinuz-$(uname -r) | grep mitigations
```

If the "mitigations" parameter is set to "off" (mitigations=off), this is a finding.

Note: The default behavior of the kernel is to enable mitigations for vulnerabilities like Meltdown and Spectre based on hardware and system requirements. Therefore, if the "mitigation" parameter is not present or if it is set to on this is not a finding.

Remediation:

Determine the default kernel:

```
$ sudo grubby --default-kernel

/boot/vmlinuz-5.4.17-2011.1.2.el8uek.x86_64
```

Using the default kernel, remove the argument that sets the Meltdown mitigations to "off":

```
$ sudo grubby --update-kernel=<path-to-default-kernel>  --remove-
args=mitigations=off
```

Reboot the system for the change to take effect.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.80 OL08-00-010430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution.

```
GROUP ID: V-248594
RULE ID: SV-248594r958928
```

Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify that OL 8 implements ASLR with the following command:

```
$ sudo sysctl kernel.randomize_va_space

kernel.randomize_va_space = 2
```

If "kernel.randomize_va_space" is not set to "2", this is a finding.

Check that the configuration files are present to enable this kernel parameter.

```
$ sudo grep -r kernel.randomize_va_space /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:kernel.randomize_va_space = 2
```

If "kernel.randomize_va_space" is not set to "2", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to implement virtual address space randomization.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.d/*.conf" (or modify the line to have the required value):

```
kernel.randomize_va_space=2
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Issue the following command to make the changes take effect:

```
$ sudo sysctl --system
```

Additional Information:

CCI-002824 Implement organization-defined controls to protect the system memory from unauthorized code execution.

- NIST SP 800-53 Revision 4::SI-16
- NIST SP 800-53 Revision 5::SI-16

Internal Only - General

1.81 OL08-00-010440 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

YUM must remove all software components after updated versions have been installed on OL 8.

```
GROUP ID: V-248595
RULE ID: SV-248595r958936
```

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

Verify the operating system removes all software components after updated versions have been installed.

Check if YUM is configured to remove unneeded packages with the following command:

```
$ sudo grep -i clean_requirements_on_remove /etc/yum.conf

clean_requirements_on_remove=True
```

If "clean_requirements_on_remove" is not set to "True", commented out, or missing from "/etc/yum.conf", this is a finding.

Remediation:

Configure OL 8 to remove all software components after updated versions have been installed.

Set the "clean_requirements_on_remove" option to "True" in the "/etc/yum.conf" file:

```
clean_requirements_on_remove=True
```

Additional Information:

CCI-002617 Remove previous versions of organization-defined software components after updated versions have been installed.

- NIST SP 800-53 Revision 4::SI-2 (6)
- NIST SP 800-53 Revision 5::SI-2 (6)

Internal Only - General

1.82 OL08-00-010450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable the SELinux targeted policy.

```
GROUP ID: V-248596
RULE ID: SV-248596r958944
```

Rationale:

Without verification of the security functions, they may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes but is not limited to establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Internal Only - General

Audit:

Ensure the operating system verifies correct operation of all security functions.

Verify that "SELinux" is active and is enforcing the targeted policy with the following command:

```
$ sudo sestatus

SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 31
```

If the "Loaded policy name" is not set to "targeted", this is a finding.

Verify that the "/etc/selinux/config" file is configured to the "SELINUXTYPE" as "targeted":

```
$ sudo grep -i "selinuxtype" /etc/selinux/config | grep -v '^#'

SELINUXTYPE = targeted
```

If no results are returned or "SELINUXTYPE" is not set to "targeted", this is a finding.

Remediation:

Configure OL 8 to verify correct operation of all security functions.

Set the "SELinuxtype" to the "targeted" policy by modifying the "/etc/selinux/config" file to have the following line:

```
SELINUXTYPE=targeted
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4::SI-6 a
- NIST SP 800-53 Revision 5::SI-6 a

Internal Only - General

1.83 OL08-00-010460 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no "shosts.equiv" files on the OL 8 operating system.

```
GROUP ID: V-248597
RULE ID: SV-248597r991589
```

Rationale:

The "shosts.equiv" files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no "shosts.equiv" files on OL 8 with the following command:

```
$ sudo find / -name shosts.equiv
```

If an "shosts.equiv" file is found, this is a finding.

Remediation:

Remove any found "shosts.equiv" files from the system.

```
$ sudo rm /etc/ssh/shosts.equiv
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.84 OL08-00-010470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no ".shosts" files on the OL 8 operating system.

```
GROUP ID: V-248598
RULE ID: SV-248598r991589
```

Rationale:

The ".shosts" files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no ".shosts" files on OL 8 with the following command:

```
$ sudo find / -name '*.shosts'
```

If any ".shosts" files are found, this is a finding.

Remediation:

Remove any found ".shosts" files from the system.

```
$ sudo rm /[path]/[to]/[file]/.shosts
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.85 OL08-00-010472 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must have the packages required to use the hardware random number generator entropy gatherer service.

```
GROUP ID: V-248600
RULE ID: SV-248600r991589
```

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (non-predictable) random number generation is important for several security functions (i.e., ciphers).

Audit:

Check that OL 8 has the packages required to enabled the hardware random number generator entropy gatherer service with the following command:

```
$ sudo yum list installed rng-tools

rng-tools.x86_64                     6.8-3.el8
@anaconda
```

If the "rng-tools" package is not installed, this is a finding.

Remediation:

Install the packages required to enabled the hardware random number generator entropy gatherer service with the following command:

```
$ sudo yum install rng-tools
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.86 OL08-00-010473 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must enable the hardware random number generator entropy gatherer service.

```
GROUP ID: V-248599
RULE ID: SV-248599r991589
```

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (nonpredictable) random number generation is important for several security functions (i.e., ciphers).

Audit:

Note: For OL versions 8.4 and above running with kernel FIPS mode enabled as specified by OL08-00-010020, this requirement is Not Applicable.

Check that OL 8 has enabled the hardware random number generator entropy gatherer service.

Verify the rngd service is enabled and active with the following commands:

```
$ sudo systemctl is-enabled rngd
 enabled

$ sudo systemctl is-active rngd
active
```

If the service is not "enabled" and "active", this is a finding.

Remediation:

Start the rngd service and enable it with the following commands:

```
$ sudo systemctl start rngd.service

$ sudo systemctl enable rngd.service
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.87 OL08-00-010480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH public host key files must have mode "0644" or less permissive.

```
GROUP ID: V-248601
RULE ID: SV-248601r991589
```

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Verify the SSH public host key files have mode "0644" or less permissive with the following command:

```
$ sudo ls -l /etc/ssh/*.pub

-rw-r--r-- 1 root wheel 618 Nov 28 06:43 ssh_host_dsa_key.pub
-rw-r--r-- 1 root wheel 347 Nov 28 06:43 ssh_host_key.pub
-rw-r--r-- 1 root wheel 238 Nov 28 06:43 ssh_host_rsa_key.pub
```

If any "key.pub" file has a mode more permissive than "0644", this is a finding.

Note: SSH public key files may be found in other directories on the system depending on the installation.

Remediation:

Change the mode of public host key files under "/etc/ssh" to "0644" with the following command:

```
$ sudo chmod 0644 /etc/ssh/*key.pub
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.88 OL08-00-010490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH private host key files must have mode "0640" or less permissive.

```
GROUP ID: V-248602
RULE ID: SV-248602r991589
```

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Audit:

Verify the SSH private host key files have mode "0640" or less permissive with the following command:

```
 $ sudo ls -alL /etc/ssh/ssh_host*key

 -rw-r----- 1 root wheel 668 Nov 28 06:43 ssh_host_dsa_key
 -rw-r----- 1 root wheel 582 Nov 28 06:43 ssh_host_key
 -rw-r----- 1 root wheel 887 Nov 28 06:43 ssh_host_rsa_key
```

If any private host key file has a mode more permissive than "0640", this is a finding.

Remediation:

Configure the mode of SSH private host key files under "/etc/ssh" to "0640" with the following command:

```
 $ sudo chmod 0640 /etc/ssh/ssh_host*key
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
 $ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.89 OL08-00-010500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH daemon must perform strict mode checking of home directory configuration files.

```
GROUP ID: V-248603
RULE ID: SV-248603r991589
```

Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Audit:

Verify the SSH daemon performs strict mode checking of home directory configuration files with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*strictmodes'

StrictModes yes
```

If "StrictModes" is set to "no" or is missing, or if the returned line is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure SSH to perform strict mode checking of home directory configuration files.

Uncomment the "StrictModes" keyword in "/etc/ssh/sshd_config" and set the value to "yes":

```
StrictModes yes
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.90 OL08-00-010520 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH daemon must not allow authentication using known host's authentication.

```
GROUP ID: V-248605
RULE ID: SV-248605r991589
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using known host’s authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*ignoreuserknownhosts'

IgnoreUserKnownHosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow authentication using known host’s authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

```
IgnoreUserKnownHosts yes
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.91 OL08-00-010521 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.

```
GROUP ID: V-248606
RULE ID: SV-248606r991589
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow Kerberos authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*kerberosauthentication'

KerberosAuthentication no
```

If the value is returned as "yes", the returned line is commented out, or no output is returned or has not been documented with the information system security officer (ISSO), this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow Kerberos authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no":

```
KerberosAuthentication no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.92 OL08-00-010522 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH daemon must not allow GSSAPI authentication, except to fulfill documented and validated mission requirements.

```
GROUP ID: V-248607
RULE ID: SV-248607r991589
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow GSSAPI authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*gssapiauthentication'

GSSAPIAuthentication no
```

If the value is returned as "yes", the returned line is commented out, or no output is returned or has not been documented with the information system security officer (ISSO), this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow GSSAPI authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no":

```
GSSAPIAuthentication no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.93 OL08-00-010540 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must use a separate file system for "/var".

```
GROUP ID: V-248608
RULE ID: SV-248608r991589
```

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system has been created for "/var" with the following command:

```
 $ sudo grep /var /etc/fstab

 /dev/mapper/...   /var   xfs   defaults,nodev 0 0
```

If a separate entry for "/var" is not in use, this is a finding.

Remediation:

Migrate the "/var" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.94 OL08-00-010541 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must use a separate file system for "/var/log".

```
GROUP ID: V-248609
RULE ID: SV-248609r991589
```

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system has been created for "/var/log".

Check that a file system has been created for "/var/log" with the following command:

```
 $ sudo grep /var/log /etc/fstab

 /dev/mapper/...   /var/log   xfs   defaults,nodev,noexec,nosuid 0 0
```

If a separate entry for "/var/log" is not in use, this is a finding.

Remediation:

Migrate the "/var/log" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.95 OL08-00-010542 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must use a separate file system for the system audit data path.

```
GROUP ID: V-248610
RULE ID: SV-248610r991589
```

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system/partition has been created for the system audit data path with the following command:

Note: "/var/log/audit" is used as the example as it is a common location.

```
$ sudo grep /var/log/audit /etc/fstab

UUID=3645951a /var/log/audit ext4 defaults 1 2
```

If an entry for "/var/log/audit" does not exist, ask the System Administrator if the system audit logs are being written to a different file system/partition on the system and then grep for that file system/partition.

If a separate file system/partition does not exist for the system audit data path, this is a finding.

Remediation:

Migrate the system audit data path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.96 OL08-00-010543 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must use a separate file system for "/tmp".

```
GROUP ID: V-248611
RULE ID: SV-248611r991589
```

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Check Text: Verify that a separate file system/partition has been created for non-privileged local interactive user home directories.

```
$ sudo grep /tmp /etc/fstab

/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If a separate entry for the file system/partition "/tmp" does not exist, this is a finding.

Remediation:

Migrate the "/tmp" directory onto a separate file system/partition.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.97 OL08-00-010544 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must use a separate file system for /var/tmp.

```
GROUP ID: V-248612
RULE ID: SV-248612r991589
```

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system has been created for "/var/tmp".

Check that a file system has been created for "/var/tmp" with the following command:

```
 $ sudo grep /var/tmp /etc/fstab

 /dev/mapper/...   /var/tmp   xfs   defaults,nodev,noexec,nosuid 0 0
```

If a separate entry for "/var/tmp" is not in use, this is a finding.

Remediation:

Migrate the "/var/tmp" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.98 OL08-00-010550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not permit direct logons to the root account using remote access via SSH.

```
GROUP ID: V-248613
RULE ID: SV-248613r1015039
```

Rationale:

Although the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Audit:

Verify remote access using SSH prevents users from logging on directly as "root" with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*permitrootlogin'

PermitRootLogin no
```

If the "PermitRootLogin" keyword is set to "yes", is missing, or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to stop users from logging on remotely as the "root" user via SSH.

Edit the appropriate "/etc/ssh/sshd_config" file to uncomment or add the line for the "PermitRootLogin" keyword and set its value to "no":

```
PermitRootLogin no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```


Internal Only - General

Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53::IA-2 (5) (b)
- NIST SP 800-53A::IA-2 (5).2 (ii)
- NIST SP 800-53 Revision 4::IA-2 (5)

Internal Only - General

1.99 OL08-00-010561 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must have the rsyslog service enabled and active.

```
GROUP ID: V-248615
RULE ID: SV-248615r991589
```

Rationale:

Configuring OL 8 to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the rsyslog service is enabled and active with the following commands:

```
$ sudo systemctl is-enabled rsyslog

enabled
$ sudo systemctl is-active rsyslog

active
```

If the service is not enabled and active, this is a finding.

Remediation:

Start and enable the rsyslog service with the following commands:

```
$ sudo systemctl start rsyslog.service
$ sudo systemctl enable rsyslog.service
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.100 OL08-00-010570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that contain user home directories.

```
GROUP ID: V-248616
RULE ID: SV-248616r991589
```

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems containing user home directories are mounted with the "nosuid" option.

Find the file system(s) that contain the user home directories with the following command:

```
$ sudo awk -F: '($3>=1000)&&($1!="nobody"){print $1,$3,$6}' /etc/passwd

smithj 1001 /home/smithj
robinst 1002 /home/robinst
```

Check the file systems that are mounted at boot time with the following command:

```
$ sudo more /etc/fstab

UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4
rw,relatime,discard,data=ordered,nosuid,nodev,noexec 0 2
```

If a file system found in "/etc/fstab" refers to the user home directory file system and it does not have the "nosuid" option set, this is a finding.

Remediation:

Configure "/etc/fstab" to use the "nosuid" option on file systems that contain user home directories for interactive users.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.101 OL08-00-010571 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent files with the setuid and setgid bit set from being executed on the /boot directory.

```
GROUP ID: V-248617
RULE ID: SV-248617r991589
```

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

For systems that use UEFI, this is Not Applicable.

Verify the /boot directory is mounted with the "nosuid" option with the following command:

```
$ sudo mount | grep '\s/boot\s'

/dev/sda1 on /boot type xfs
(rw,nosuid,relatime,seclabe,attr2,inode64,noquota)
```

If the /boot file system does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on the /boot directory.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.102 OL08-00-010572 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent files with the setuid and setgid bit set from being executed on the /boot/efi directory.

```
GROUP ID: V-248618
RULE ID: SV-248618r991589
```

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

For systems that use BIOS, this is Not Applicable.

Verify the /boot/efi directory is mounted with the "nosuid" option with the following command:

```
$ sudo mount | grep '\s/boot/efi\s'

/dev/sda1 on /boot/efi type vfat
(rw,nosuid,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=ascii,shortn
ame=winnt,errors=remount-ro)
```

If the /boot/efi file system does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on the /boot/efi directory.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.103 OL08-00-010580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent special devices on non-root local partitions.

```
GROUP ID: V-248619
RULE ID: SV-248619r991589
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access. The only legitimate location for device files is the /dev directory located on the root partition.

Audit:

Verify all non-root local partitions are mounted with the "nodev" option with the following command:

```
$ sudo mount | grep '^/dev\S* on /\S' | grep --invert-match 'nodev'
```

If any output is produced, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on all non-root local partitions.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.104 OL08-00-010590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 file systems that contain user home directories must not execute binary files.

```
GROUP ID: V-248620
RULE ID: SV-248620r991589
```

Rationale:

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems containing user home directories are mounted with the "noexec" option.

Find the file system(s) that contain the user home directories with the following command:

```
$ sudo awk -F: '($3>=1000)&&($1!="nobody"){print $1,$3,$6}' /etc/passwd

smithj 1001 /home/smithj
robinst 1002 /home/robinst
```

Check the file systems that are mounted at boot time with the following command:

```
$ sudo more /etc/fstab

UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4
rw,relatime,discard,data=ordered,nosuid,nodev,noexec 0 2
```

If a file system found in "/etc/fstab" refers to the user home directory file system and it does not have the "noexec" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that contain user home directories for interactive users.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.105 OL08-00-010600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 file systems must not interpret character or block special devices from untrusted file systems.

```
GROUP ID: V-248621
RULE ID: SV-248621r991589
```

Rationale:

The "nodev" mount option causes the system not to interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems used for removable media are mounted with the "nodev" option with the following command:

```
$ sudo more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to removable media and it does not have the "nodev" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on file systems that are associated with removable media.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.106 OL08-00-010610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 file systems must not execute binary files on removable media.

```
GROUP ID: V-248622
RULE ID: SV-248622r991589
```

Rationale:

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems used for removable media are mounted with the "noexec" option with the following command:

```
$ sudo more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to removable media and it does not have the "noexec" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that are associated with removable media.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.107 OL08-00-010620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that are used with removable media.

```
GROUP ID: V-248623
RULE ID: SV-248623r991589
```

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems used for removable media are mounted with the "nosuid" option with the following command:

```
$ sudo more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to removable media and it does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on file systems that are associated with removable media.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.108 OL08-00-010630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 file systems must not execute binary files that are imported via Network File System (NFS).

```
GROUP ID: V-248624
RULE ID: SV-248624r991589
```

Rationale:

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems being imported via NFS are mounted with the "noexec" option with the following command:

```
$ sudo grep nfs /etc/fstab | grep noexec

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0
0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "noexec" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that are being imported via NFS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.109 OL08-00-010640 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 file systems must not interpret character or block special devices that are imported via NFS.

```
GROUP ID: V-248625
RULE ID: SV-248625r991589
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems being imported via NFS are mounted with the "nodev" option with the following command:

```
$ sudo grep nfs /etc/fstab | grep nodev

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0
0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "nodev" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on file systems that are being imported via NFS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.110 OL08-00-010650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).

```
GROUP ID: V-248626
RULE ID: SV-248626r991589
```

Rationale:

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify that file systems being imported via NFS are mounted with the "nosuid" option with the following command:

```
$ sudo grep nfs /etc/fstab | grep nosuid

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0
0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "nosuid" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on file systems that are being imported via NFS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.111 OL08-00-010660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Local OL 8 initialization files must not execute world-writable programs.

```
GROUP ID: V-248627
RULE ID: SV-248627r991589
```

Rationale:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Audit:

Verify that local initialization files do not execute world-writable programs.

Check the system for world-writable files.

The following command will discover and print world-writable files. Run it once for each local partition [PART]:

```
$ sudo find [PART] -xdev -type f -perm -0002 -print
```

For all files listed, check for their presence in the local initialization files with the following commands:

Note: The example will be for a system that is configured to create users' home directories in the "/home" directory.

```
$ sudo grep <file> /home/*/.*
```

If any local initialization files are found to reference world-writable files, this is a finding.

Remediation:

Set the mode on files being executed by the local initialization files with the following command:

```
$ sudo chmod 0755 <file>
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.112 OL08-00-010670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable kernel dumps unless needed.

```
GROUP ID: V-248628
RULE ID: SV-248628r991562
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

OL 8 installation media presents the option to enable or disable the kdump service at the time of system installation.

Audit:

Verify that kernel core dumps are disabled unless needed with the following command:

```
$ sudo systemctl status kdump.service

kdump.service - Crash recovery kernel arming
Loaded: loaded (/usr/lib/systemd/system/kdump.service; disabled; vendor
preset: enabled)
Active: failed (Result: exit-code)since Mon 2020-05-04 16:08:09 EDT; 3min ago
Main PID: 1130 (code=exited, status=0/FAILURE)
```

If the "kdump" service is active, ask the System Administrator if the use of the service is required and documented with the Information System Security Officer (ISSO).

If the service is active and is not documented, this is a finding.

Remediation:

If kernel core dumps are not required, disable the "kdump" service with the following command:

```
$ sudo systemctl disable kdump.service
```

If kernel core dumps are required, document the need with the ISSO.

Internal Only - General

Additional Information:

CCI-001665 Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (v)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-24

Internal Only - General

1.113 OL08-00-010671 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable the "kernel.core_pattern".

```
GROUP ID: V-248629
RULE ID: SV-248629r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify that OL 8 disables storing core dumps with the following commands:

```
$ sudo sysctl kernel.core_pattern

kernel.core_pattern = |/bin/false
```

If the returned line does not have a value of "|/bin/false", or a line is not returned and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Check that the configuration files are present to enable this kernel parameter:

```
$ sudo grep -r kernel.core_pattern /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf:kernel.core_pattern = |/bin/false
```

If "kernel.core_pattern" is not set to "|/bin/false", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable storing core dumps by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.core_pattern = |/bin/false
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.114 OL08-00-010672 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable acquiring, saving, and processing core dumps.

```
GROUP ID: V-248630
RULE ID: SV-248630r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

When the kernel invokes "systemd-coredump" to handle a core dump, it runs in privileged mode and will connect to the socket created by the "systemd-coredump.socket" unit. This, in turn, will spawn an unprivileged "systemd-coredump@.service" instance to process the core dump.

Audit:

Verify OL 8 is not configured to acquire, save, or process core dumps with the following command:

```
$ sudo systemctl status systemd-coredump.socket

systemd-coredump.socket
Loaded: masked (Reason: Unit systemd-coredump.socket is masked.)
Active: inactive (dead)
```

If the "systemd-coredump.socket" is loaded and not masked and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure the system to disable the "systemd-coredump.socket" with the following commands:

```
$ sudo systemctl disable --now systemd-coredump.socket
$ sudo systemctl mask systemd-coredump.socket

Created symlink /etc/systemd/system/systemd-coredump.socket -> /dev/null
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.115 OL08-00-010673 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable core dumps for all users.

```
GROUP ID: V-248631
RULE ID: SV-248631r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify the operating system disables core dumps for all users with the following command:

```
$ sudo grep -r -s '^[^#].*core' /etc/security/limits.conf
/etc/security/limits.d/*.conf

* hard core 0
```

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.

If the "core" item is missing or commented out or the value is anything other than "0", and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure OL 8 to disable core dumps for all users.

Add the following line to the top of "/etc/security/limits.conf" or in a ".conf" file defined in "/etc/security/limits.d/":

```
* hard core 0
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.116 OL08-00-010674 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable storing core dumps.

```
GROUP ID: V-248632
RULE ID: SV-248632r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify the operating system disables storing core dumps for all users with the following command:

```
$ sudo grep -i storage /etc/systemd/coredump.conf

Storage=none
```

If the "Storage" item is missing or commented out or the value is anything other than "none", and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure OL 8 to disable storing core dumps for all users.

Add or modify the following line in "/etc/systemd/coredump.conf":

```
Storage=none
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.117 OL08-00-010675 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable core dump backtraces.

```
GROUP ID: V-248633
RULE ID: SV-248633r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify the operating system disables core dump backtraces by issuing the following command:

```
$ sudo grep -i ProcessSizeMax /etc/systemd/coredump.conf

ProcessSizeMax=0
```

If the "ProcessSizeMax" item is missing or commented out or the value is anything other than "0", and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure OL 8 to disable core dump backtraces.

Add or modify the following line in "/etc/systemd/coredump.conf":

```
ProcessSizeMax=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.118 OL08-00-010680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

For OL 8 systems using Domain Name Servers (DNS) resolution, at least two name servers must be configured.

```
GROUP ID: V-248634
RULE ID: SV-248634r991589
```

Rationale:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Audit:

Determine whether the system is using local or DNS name resolution with the following command:

```
$ sudo grep hosts /etc/nsswitch.conf

hosts: files dns
```

If the DNS entry is missing from the host's line in the "/etc/nsswitch.conf" file, the "/etc/resolv.conf" file must be empty.

Verify the "/etc/resolv.conf" file is empty with the following command:

```
$ sudo ls -al /etc/resolv.conf

-rw-r--r-- 1 root root 0 Aug 19 08:31 resolv.conf
```

If local host authentication is being used and the "/etc/resolv.conf" file is not empty, this is a finding.

If the DNS entry is found on the host's line of the "/etc/nsswitch.conf" file, verify the operating system is configured to use two or more name servers for DNS resolution.

Determine the name servers used by the system with the following command:

```
$ sudo grep nameserver /etc/resolv.conf

nameserver 192.168.1.2
nameserver 192.168.1.3
```

If fewer than two lines are returned that are not commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to use two or more name servers for DNS resolution.

By default, "NetworkManager" on OL 8 dynamically updates the "/etc/resolv.conf" file with the DNS settings from active "NetworkManager" connection profiles. However, this feature can be disabled to allow manual configurations.

If manually configuring DNS, edit the "/etc/resolv.conf" file to uncomment or add the two or more "nameserver" option lines with the IP address of local authoritative name servers.

If local host resolution is being performed, the "/etc/resolv.conf" file must be empty. An empty "/etc/resolv.conf" file can be created as follows:

```
$ sudo echo -n > /etc/resolv.conf
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.119 OL08-00-010690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Executable search paths within the initialization files of all local interactive OL 8 users must only contain paths that resolve to the system default or the user's home directory.

```
GROUP ID: V-248635
RULE ID: SV-248635r991589
```

Rationale:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands.

This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Audit:

Verify that all local interactive user initialization files' executable search path statements do not contain statements that will reference a working directory other than the users' home directory with the following commands:

Note: The example will be for the "smithj" user, which has a home directory of "/home/smithj".

```
$ sudo grep -i path /home/smithj/.*

/home/smithj/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/bin
/home/smithj/.bash_profile:export PATH
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory, this is a finding.

Remediation:

Edit the local interactive user initialization files to change any PATH variable statements that reference directories other than their home directory.

If a local interactive user requires path variables to reference a directory owned by the application, it must be documented with the ISSO.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.120 OL08-00-010700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 world-writable directories must be owned by root, sys, bin, or an application user.

```
GROUP ID: V-248636
RULE ID: SV-248636r991589
```

Rationale:

If a world-writable directory is not owned by root, sys, bin, or an application User Identifier (UID), unauthorized users may be able to modify files created by others.

The only authorized public directories are the temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

The following command will discover and print world-writable directories that are not owned by a system account, given the assumption that only system accounts have a UID lower than 1000. Run it once for each local partition [PART]:

```
$ sudo find [PART] -xdev -type d -perm -0002 -uid +999 -print
```

If there is output, this is a finding.

Remediation:

Investigate any world-writable directories that are not owned by a system account and then delete the files or assign them to an appropriate group.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.121 OL08-00-010710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 world-writable directories must be group-owned by root, sys, bin, or an application group.

```
GROUP ID: V-248637
RULE ID: SV-248637r991589
```

Rationale:

If a world-writable directory is not group-owned by root, sys, bin, or an application Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are the temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

The following command will discover and print world-writable directories that are not group-owned by a system account, given the assumption that only system accounts have a gid lower than 1000. Run it once for each local partition [PART]:

```
$ sudo find [PART] -xdev -type d -perm -0002 -gid +999 -print
```

If there is output, this is a finding.

Remediation:

Investigate any world-writable directories that are not group-owned by a system account and then delete the files or assign them to an appropriate group.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.122 OL08-00-010720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local interactive users must have a home directory assigned in the "/etc/passwd" file.

```
GROUP ID: V-248638
RULE ID: SV-248638r991589
```

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify local interactive users on OL 8 have a home directory assigned with the following command:

```
$ sudo pwck -r

user 'lp': directory '/var/spool/lpd' does not exist
user 'news': directory '/var/spool/news' does not exist
user 'uucp': directory '/var/spool/uucp' does not exist
user 'www-data': directory '/var/www' does not exist
```

Ask the System Administrator (SA) if any users found without home directories are local interactive users.

If the SA is unable to provide a response, check for users with a User Identifier (UID) of 1000 or greater with the following command:

```
$ sudo awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1, $3, $6}' /etc/passwd
```

If any interactive users do not have a home directory assigned, this is a finding.

Remediation:

Assign home directories to all local interactive users on OL 8 that currently do not have a home directory assigned.

Additional Information:
CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.123 OL08-00-010730 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local interactive user home directories must have mode "0750" or less permissive.

```
GROUP ID: V-248639
RULE ID: SV-248639r991589
```

Rationale:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Audit:

Verify the assigned home directory of all local interactive users has a mode of "0750" or less permissive with the following command.

Note: This may miss interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.

```
$ sudo ls -ld $(awk -F: '($3>=1000)&&($1!="nobody"){print $6}' /etc/passwd)

drwxr-x--- 2 smithj admin 4096 Jun 5 12:41 smithj
```

If home directories of interactive users referenced in "/etc/passwd" do not have a mode of "0750" or less permissive, this is a finding.

Remediation:

Change the mode of interactive users' home directories to "0750" using the following command.

Note: The example will be for the user "smithj".

```
$ sudo chmod 0750 /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.124 OL08-00-010731 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local interactive user home directory files must have mode "0750" or less permissive.

```
GROUP ID: V-248640
RULE ID: SV-248640r991589
```

Rationale:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Audit:

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750".

Files that begin with a "." are excluded from this requirement.

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
$ sudo ls -lLR /home/smithj

-rwxr-x--- 1 smithj smithj 18 Mar 5 17:06 file1
-rwxr----- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r-x--- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files or directories are found with a mode more permissive than "0750", this is a finding.

Remediation:

Set the mode on files and directories in the local interactive user home directory with the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
$ sudo chmod 0750 /home/smithj/<file or directory>
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.125 OL08-00-010740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local interactive user home directories must be group-owned by the home directory owner's primary group.

```
GROUP ID: V-248641
RULE ID: SV-248641r991589
```

Rationale:

If the Group Identifier (GID) of a local interactive user’s home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user’s files. Users that share the same group may not be able to access files to which they legitimately should have access.

Audit:

Verify the assigned home directory of all local interactive users is group-owned by that user’s primary GID with the following command.

Note: This may miss local interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information. The returned directory "/home/smithj" is used as an example.

```
$ sudo ls -ld $(awk -F: '($3>=1000)&&($1!="nobody"){print $6}' /etc/passwd)

drwxr-x--- 2 smithj admin 4096 Jun 5 12:41 smithj
```

Check the user's primary group with the following command:

```
$ sudo grep $(grep smithj /etc/passwd | awk -F: '{print $4}') /etc/group

admin:x:250:smithj,jonesj,jacksons
```

If the user home directory referenced in "/etc/passwd" is not group-owned by that user’s primary GID, this is a finding.

Internal Only - General

Remediation:

Change the group owner of a local interactive user's home directory to the group found in "/etc/passwd" using the following command.

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj" and has a primary group of users.

```
$ sudo chgrp users /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.126 OL08-00-010760 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local interactive user accounts must be assigned a home directory upon creation.

```
GROUP ID: V-248644
RULE ID: SV-248644r991589
```

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify all local interactive users on OL 8 are assigned a home directory upon creation with the following command:

```
$ sudo grep -i create_home /etc/login.defs

CREATE_HOME yes
```

If the value for "CREATE_HOME" parameter is not set to "yes", the line is missing, or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to assign home directories to all new local interactive users by setting the "CREATE_HOME" parameter in "/etc/login.defs" to "yes" as follows.

```
CREATE_HOME yes
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.127 OL08-00-010750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local interactive user home directories defined in the "/etc/passwd" file must exist.

```
GROUP ID: V-248643
RULE ID: SV-248643r991589
```

Rationale:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the "/" directory as the current working directory upon logon. This could create a denial of service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Audit:

Verify that the assigned home directory of all local interactive users on OL 8 exists with the following command:

```
$ sudo ls -ld $(awk -F: '($3>=1000)&&($1!="nobody"){print $6}' /etc/passwd)

drwxr-xr-x 2 smithj admin 4096 Jun 5 12:41 smithj
```

Note: This may miss interactive users that have been assigned a privileged User ID (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check that all referenced home directories exist with the following command:

```
$ sudo pwck -r

user 'smithj': directory '/home/smithj' does not exist
```

If any home directories referenced in "/etc/passwd" are returned as not defined, this is a finding.

Internal Only - General

Remediation:

Create home directories to all local interactive users that currently do not have a home directory assigned. Use the following commands to create the user home directory assigned in "/etc/ passwd".

Note: The example will be for the user smithj, who has a home directory of "/home/smithj", a UID of "smithj", and a Group Identifier (GID) of "users assigned" in "/etc/passwd".

```
$ sudo mkdir /home/smithj
$ sudo chown smithj /home/smithj
$ sudo chgrp users /home/smithj
$ sudo chmod 0750 /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.128 OL08-00-010741 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

```
GROUP ID: V-248642
RULE ID: SV-248642r991589
```

Rationale:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Audit:

Verify all files and directories in a local interactive user home directory are group-owned by a group that the user is a member.

Check the group owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
$ sudo ls -lLR /<home directory>/<users home directory>/

-rw-r--r-- 1 smithj smithj  18 Mar  5 17:06 file1
-rw-r--r-- 1 smithj smithj 193 Mar  5 17:06 file2
-rw-r--r-- 1 smithj sa        231 Mar  5 17:06 file3
```

If any files found with a group-owner different from the home directory user private group, determine if the user is a member of that group with the following command:

```
$ sudo grep smithj /etc/group

sa:x:100:juan,shelley,bob,smithj
smithj:x:521:smithj
```

If any files or directories are group owned by a group that the directory owner is not a member of, this is a finding.

Internal Only - General

Remediation:

Change the group of a local interactive user's files and directories to a group that the interactive user is a member. To change the group owner of a local interactive user's files and directories, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
$ sudo chgrp smithj /home/smithj/<file or directory>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.129 OL08-00-010780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 files and directories must have a valid owner.

```
GROUP ID: V-248646
RULE ID: SV-248646r991589
```

Rationale:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier "UID" as the UID of the unowned files.

Audit:

Verify all files and directories on OL 8 have a valid owner with the following command:

```
$ sudo find / -nouser
```

If any files on the system do not have an assigned owner, this is a finding.

Remediation:

Either remove all files and directories from the system that do not have a valid user or assign a valid user to all unowned files and directories on OL 8 with the "chown" command:

```
$ sudo chown <user> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.130 OL08-00-010790 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 files and directories must have a valid group owner.

```
GROUP ID: V-248647
RULE ID: SV-248647r991589
```

Rationale:

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Audit:

Verify all files and directories on OL 8 have a valid group with the following command:

```
$ sudo find / -nogroup
```

If any files on the system do not have an assigned group, this is a finding.

Remediation:

Either remove all files and directories from OL 8 that do not have a valid group, or assign a valid group to all files and directories on the system with the "chgrp" command:

```
$ sudo chgrp <group> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.131 OL08-00-010770 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 local initialization files must have mode "0740" or less permissive.

```
GROUP ID: V-248645
RULE ID: SV-248645r991589
```

Rationale:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify that all local initialization files have a mode of "0740" or less permissive with the following command:

Note: The example will be for the "smithj" user, who has a home directory of "/home/smithj".

```
$ sudo ls -al /home/smithj/.* | more

-rwxr----- 1 smithj users 896 Mar 10 2011 .profile
-rwxr----- 1 smithj users 497 Jan 6 2007 .login
-rwxr----- 1 smithj users 886 Jan 6 2007 .something
```

If any local initialization files have a mode more permissive than "0740", this is a finding.

Remediation:

Set the mode of the local initialization files to "0740" with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

```
$ sudo chmod 0740 /home/smithj/.<INIT_FILE>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.132 OL08-00-010820 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Unattended or automatic logon via the OL 8 graphical user interface must not be allowed.

```
GROUP ID: V-248649
RULE ID: SV-248649r991591
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.

Check for the value of "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

```
$ sudo grep -i automaticloginenable /etc/gdm/custom.conf

AutomaticLoginEnable=false
```

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

Remediation:

Configure OL 8 to not allow an unattended or automatic logon to the system via a graphical user interface.

Add or edit the line for the "AutomaticLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

```
[daemon]
AutomaticLoginEnable=false
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.133 OL08-00-010800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A separate OL 8 filesystem must be used for user home directories (such as "/home" or an equivalent).

```
GROUP ID: V-248648
RULE ID: SV-248648r991589
```

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system has been created for non-privileged local interactive user home directories.

Check the home directory assignment for all non-privileged users, users with a User Identifier (UID) greater than 1000, on the system with the following command:

```
$ sudo awk -F: '($3>=1000)&&($1!="nobody"){print $1,$3,$6}' /etc/passwd

doej 1001 /home/doej
publicj 1002 /home/publicj
smithj 1003 /home/smithj
```

The output of the command will give the directory that contains the home directories for the nonprivileged users on the system (in this example, "/home") and users' shell. All accounts with a valid shell (such as "/bin/bash") are considered interactive users.

Check that a file system has been created for the nonprivileged interactive users with the following command.

Note: The partition of "/home" is used in the example.

```
$ sudo grep /home /etc/fstab

/dev/mapper/...   /home   xfs   defaults,noexec,nosuid,nodev 0 0
```

If a separate entry for the file system that contains the nonprivileged interactive users' home directories does not exist, this is a finding.

Remediation:

Migrate the "/home" directory onto a separate file system.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.134 OL08-00-010830 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must not allow users to override SSH environment variables.

```
GROUP ID: V-248650
RULE ID: SV-248650r991591
```

Rationale:

SSH environment options potentially allow users to bypass access restriction in some configurations.

Audit:

Verify that unattended or automatic login via SSH is disabled with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*permituserenvironment'

PermitUserEnvironment no
```

If "PermitUserEnvironment" is set to "yes", is missing completely, or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to allow the SSH daemon to not allow unattended or automatic login to the system.

Add or edit the following line in the "/etc/ssh/sshd_config" file:

```
PermitUserEnvironment no
```

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.135 OL08-00-020000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 temporary user accounts must be provisioned with an expiration time of 72 hours or less.

```
GROUP ID: V-248651
RULE ID: SV-248651r958364
```

Rationale:

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, OL 8 must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many OL 8 operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify that temporary accounts have been provisioned with an expiration date of 72 hours.

For every existing temporary account, run the following command to obtain its account expiration information.

```
$ sudo chage -l system_account_name
```

Verify each of these accounts has an expiration date set within 72 hours.

If any temporary accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Internal Only - General

Remediation:

If a temporary account must be created, configure the system to terminate the account after a 72-hour time period with the following command to set an expiration date on it.

Substitute "system_account_name" with the account to be created.

```
$ sudo chage -E `date -d "+3 days" +%Y-%m-%d` system_account_name
```

Additional Information:

CCI-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53 Revision 5::AC-2 (2)

Internal Only - General

1.136 OL08-00-020010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must automatically lock an account when three unsuccessful logon attempts occur.

```
GROUP ID: V-248652
RULE ID: SV-248652r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the system locks an account after three unsuccessful logon attempts with the following commands.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "deny" option is not set to "3" or less (but not "0") on the "preauth" line with the "pam_faillock.so" module or is missing from this line, this is a finding.

If any line referencing the "pam_faillock.so" module is commented out, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "deny" option is not set to "3" or less (but not "0") on the "preauth" line with the "pam_faillock.so" module or is missing from this line, this is a finding.

If any line referencing the "pam_faillock.so" module is commented out, this is a finding.

Remediation:

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.137 OL08-00-020011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must automatically lock an account when three unsuccessful logon attempts occur.

```
GROUP ID: V-248653
RULE ID: SV-248653r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts:

```
$ sudo grep 'deny =' /etc/security/faillock.conf

deny = 3
```

If the "deny" option is not set to "3" or less (but not "0") or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to lock an account when three unsuccessful logon attempts occur.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
deny = 3
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.138 OL08-00-020012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-248654
RULE ID: SV-248654r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the system locks an account after three unsuccessful logon attempts within a period of 15 minutes with the following commands.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "fail_interval" option is not set to "900" or more on the "preauth" lines with the "pam_faillock.so" module or is missing from this line, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "fail_interval" option is not set to "900" or more on the "preauth" lines with the "pam_faillock.so" module or is missing from this line, this is a finding.

Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur in 15 minutes.

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.139 OL08-00-020013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-248655
RULE ID: SV-248655r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes:

```
$ sudo grep 'fail_interval =' /etc/security/faillock.conf

fail_interval = 900
```

If the "fail_interval" option is not set to "900" or more or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to lock an account when three unsuccessful logon attempts occur.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
fail_interval = 900
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.140 OL08-00-020014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-248656
RULE ID: SV-248656r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator with the following commands.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "unlock_time" option is not set to "0" on the "preauth" and "authfail" lines with the "pam_faillock.so" module or is missing from these lines, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "unlock_time" option is not set to "0" on the "preauth" and "authfail" lines with the "pam_faillock.so" module or is missing from these lines, this is a finding.

Remediation:

Configure the operating system to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.141 OL08-00-020015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-248657
RULE ID: SV-248657r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts:

```
$ sudo grep 'unlock_time =' /etc/security/faillock.conf

unlock_time = 0
```

If the "unlock_time" option is not set to "0" or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
unlock_time = 0
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.142 OL08-00-020016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must ensure account lockouts persist.

```
GROUP ID: V-248658
RULE ID: SV-248658r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the faillock directory contents persist after a reboot with the following commands:

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "dir" option is not set to a non-default documented tally log directory on the "preauth" and "authfail" lines with the "pam_faillock.so" module or is missing from these lines, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "dir" option is not set to a non-default documented tally log directory on the "preauth" and "authfail" lines with the "pam_faillock.so" module or is missing from these lines, this is a finding.

Internal Only - General

Remediation:

Configure the operating system maintain the contents of the faillock directory after a reboot.

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines.

Note: Using the default faillock directory of "/var/run/faillock" will result in the contents being cleared in the event of a reboot.

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.143 OL08-00-020017 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must ensure account lockouts persist.

```
GROUP ID: V-248659
RULE ID: SV-248659r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured use a non-default faillock directory to ensure contents persist after reboot:

```
$ sudo grep 'dir =' /etc/security/faillock.conf

dir = /var/log/faillock
```

If the "dir" option is not set to a non-default documented tally log directory or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to maintain the contents of the faillock directory after a reboot.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
dir = /var/log/faillock
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.144 OL08-00-020018 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must prevent system messages from being presented when three unsuccessful logon attempts occur.

```
GROUP ID: V-248660
RULE ID: SV-248660r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the system prevents informative messages from being presented to the user pertaining to logon information with the following commands.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "silent" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "silent" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

Remediation:

Configure the operating system to prevent informative messages from being presented at logon attempts.

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.145 OL08-00-020019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must prevent system messages from being presented when three unsuccessful logon attempts occur.

```
GROUP ID: V-248661
RULE ID: SV-248661r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the" pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to prevent informative messages from being presented at logon attempts:

```
$ sudo grep silent /etc/security/faillock.conf

silent
```

If the "silent" option is not set or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to prevent informative messages from being presented at logon attempts.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
silent
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.146 OL08-00-020020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must log user name information when unsuccessful logon attempts occur.

```
GROUP ID: V-248662
RULE ID: SV-248662r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the system logs user name information when unsuccessful logon attempts occur with the following commands.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "audit" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "audit" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

Remediation:

Configure the operating system to log user name information when unsuccessful logon attempts occur.

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.147 OL08-00-020021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must log user name information when unsuccessful logon attempts occur.

```
GROUP ID: V-248663
RULE ID: SV-248663r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur:

```
$ sudo grep audit /etc/security/faillock.conf

audit
```

If the "audit" option is not set, is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to log user name information when unsuccessful logon attempts occur.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
audit
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.148 OL08-00-020022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-248664
RULE ID: SV-248664r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

OL 8 can use the "pam_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Verify the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes with the following commands.

Note: If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "even_deny_root" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "even_deny_root" option is missing from the "preauth" line with the "pam_faillock.so" module, this is a finding.

Remediation:

Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes.

Add/modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.149 OL08-00-020023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-248665
RULE ID: SV-248665r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2, the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam_faillock.so" module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur:

```
$ sudo grep even_deny_root /etc/security/faillock.conf

even_deny_root
```

If the "even_deny_root" option is not set or is missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes.

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
even_deny_root
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.150 OL08-00-020024 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must limit the number of concurrent sessions to 10 for all accounts and/or account types.

```
GROUP ID: V-248666
RULE ID: SV-248666r958398
```

Rationale:

Operating system management includes the ability to control the number of users and user sessions that use an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to denial-of-service attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

Verify the operating system limits the number of concurrent sessions to 10 for all accounts and/or account types by issuing the following command:

```
$ sudo grep "maxlogins" /etc/security/limits.conf
/etc/security/limits.d/*.conf

* hard maxlogins 10
```

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.

If the "maxlogins" item is missing or commented out, or the value is not set to "10" or less for all domains that have the "maxlogins" item assigned, this is a finding.

Remediation:

Configure OL 8 to limit the number of concurrent sessions to 10 for all accounts and/or account types.

Add the following line to the top of "/etc/security/limits.conf" or in a ".conf" file defined in "/etc/security/limits.d/":

```
* hard maxlogins 10
```


Internal Only - General

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

Internal Only - General

1.151 OL08-00-020025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must configure the use of the pam_faillock.so module in the /etc/pam.d/system-auth file.

```
GROUP ID: V-248667
RULE ID: SV-248667r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2 the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The preauth argument must be used when the module is called before the modules that ask for user credentials, such as the password.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Audit:

Note: This check applies to OL versions 8.2 or newer, if the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the pam_faillock.so module is present in the "/etc/pam.d/system-auth" file:

```
$ sudo grep pam_faillock.so /etc/pam.d/system-auth

auth               required                                pam_faillock.so preauth
auth               required                                pam_faillock.so
authfail
account          required                              pam_faillock.so
```

If the pam_faillock.so module is not present in the "/etc/pam.d/system-auth" file with the "preauth" line listed before pam_unix.so, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to include the use of the pam_faillock.so module in the /etc/pam.d/system-auth file.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" file to match the following lines:

Note: The "preauth" line must be listed before pam_unix.so.

```
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.152 OL08-00-020026 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must configure the use of the pam_faillock.so module in the /etc/pam.d/password-auth file.

```
GROUP ID: V-248668
RULE ID: SV-248668r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In OL 8.2 the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam_faillock.so module. Also introduced is a "local_users_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The preauth argument must be used when the module is called before the modules that ask for user credentials, such as the password.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

Note: This check applies to OL versions 8.2 or newer, if the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the pam_faillock.so module is present in the "/etc/pam.d/password-auth" file:

```
$ sudo grep pam_faillock.so /etc/pam.d/password-auth

auth                required                                pam_faillock.so
preauth
auth                required                                pam_faillock.so
authfail
account           required                              pam_faillock.so
```

If the pam_faillock.so module is not present in the "/etc/pam.d/password-auth" file with the "preauth" line listed before pam_unix.so, this is a finding.

Remediation:

Configure the operating system to include the use of the pam_faillock.so module in the /etc/pam.d/password-auth file.

Add/Modify the appropriate sections of the "/etc/pam.d/password-auth" file to match the following lines:

Note: The "preauth" line must be listed before pam_unix.so.

```
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.153 OL08-00-020027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, versions 8.2 and above, must configure SELinux context type to allow the use of a non-default faillock tally directory.

```
GROUP ID: V-248669
RULE ID: SV-248669r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

From "faillock.conf" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be re-enabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

SELinux, enforcing a targeted policy, will require any non-default tally directory's security context type to match the default directory's security context type. Without updating the security context type, the pam_faillock module will not write failed login attempts to the non-default tally directory.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

If the system does not have SELinux enabled and enforcing a targeted policy, or if the pam_faillock module is not configured for use, this requirement is not applicable.

Note: This check applies to OL versions 8.2 or newer. If the system is OL version 8.0 or 8.1, this check is not applicable.

Verify the location of the non-default tally directory for the pam_faillock module with the following command:

```
$ sudo grep -w dir /etc/security/faillock.conf

dir = /var/log/faillock
```

Check the security context type of the non-default tally directory with the following command:

```
$ sudo ls -Zd /var/log/faillock

unconfined_u:object_r:faillog_t:s0 /var/log/faillock
```

If the security context type of the non-default tally directory is not "faillog_t", this is a finding.

Remediation:

Configure OL 8 to allow the use of a non-default faillock tally directory while SELinux enforces a targeted policy.

Create a non-default faillock tally directory (if it does not already exist) with the following example:

```
$ sudo mkdir /var/log/faillock
```

Update the /etc/selinux/targeted/contexts/files/file_contexts.local with "faillog_t" context type for the non-default faillock tally directory with the following command:

```
$ sudo semanage fcontext -a -t faillog_t "/var/log/faillock(/.*)?"
```

Next, update the context type of the non-default faillock directory/subdirectories and files with the following command:

```
$ sudo restorecon -R -v /var/log/faillock
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.154 OL08-00-020028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.2 must configure SELinux context type to allow the use of a non-default faillock tally directory.

```
GROUP ID: V-248670
RULE ID: SV-248670r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

From "Pam_Faillock" man pages: Note that the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

SELinux, enforcing a targeted policy, will require any non-default tally directory's security context type to match the default directory's security context type. Without updating the security context type, the pam_faillock module will not write failed login attempts to the non-default tally directory.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

Internal Only - General

Audit:

If the system does not have SELinux enabled and enforcing a targeted policy, or if the pam_faillock module is not configured for use, this requirement is not applicable.

Note: This check applies to OL versions 8.0 and 8.1. If the system is OL version 8.2 or newer, this check is not applicable.

Verify the location of the non-default tally directory for the pam_faillock module with the following command:

```
$ sudo grep -w dir /etc/pam.d/password-auth

auth   required   pam_faillock.so preauth dir=/var/log/faillock
auth   required   pam_faillock.so authfail dir=/var/log/faillock
```

Check the security context type of the non-default tally directory with the following command:

```
$ sudo ls -Zd /var/log/faillock

unconfined_u:object_r:faillog_t:s0 /var/log/faillock
```

If the security context type of the non-default tally directory is not "faillog_t", this is a finding.

Remediation:

Configure OL 8 to allow the use of a non-default faillock tally directory while SELinux enforces a targeted policy.

Update the /etc/selinux/targeted/contexts/files/file_contexts.local with "faillog_t" context type for the non-default faillock tally directory with the following command:

```
$ sudo semanage fcontext -a -t faillog_t "/var/log/faillock(/.*)?"
```

Next, update the context type of the non-default faillock directory/subdirectories and files with the following command:

```
$ sudo restorecon -R -v /var/log/faillock
```


Internal Only - General

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

Internal Only - General

1.155 OL08-00-020030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable a user session lock until that user reestablishes access using established identification and authentication procedures for graphical user sessions.

```
GROUP ID: V-248671
RULE ID: SV-248671r1015040
```

Rationale:

To establish acceptance of the application usage policy, a click-through banner at system logon is required. The system must prevent further activity until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system enables a user's session lock until that user reestablishes access using established identification and authentication procedures with the following command:

```
$ sudo gsettings get org.gnome.desktop.screensaver lock-enabled

true
```

If the setting is "false", this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to enable a user's session lock until that user reestablishes access using established identification and authentication procedures.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following example:

```
$ sudo vi /etc/dconf/db/local.d/00-screensaver
```

Edit the "[org/gnome/desktop/screensaver]" section of the database file and add or update the following lines:

```
# Set this to true to lock the screen when the screensaver activates
lock-enabled=true
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

Internal Only - General

1.156 OL08-00-020031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must initiate a session lock for graphical user interfaces when the screensaver is activated.

```
GROUP ID: V-248672
RULE ID: SV-248672r958402
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated with the following command:

```
$ sudo gsettings get org.gnome.desktop.screensaver lock-delay

uint32 5
```

If the "uint32" setting is missing, or is not set to "5" or less, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to initiate a session lock for graphical user interfaces when a screensaver is activated.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/00-screensaver
[org/gnome/desktop/screensaver]
lock-delay=uint32 5
```

The "uint32" must be included along with the integer key values as shown.

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.157 OL08-00-020032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable the user list at logon for graphical user interfaces.

```
GROUP ID: V-248673
RULE ID: SV-248673r991589
```

Rationale:

Leaving the user list enabled is a security risk since it allows anyone with physical access to the system to enumerate known user accounts without authenticated access to the system.

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system disables the user logon list for graphical user interfaces with the following command:

```
$ sudo gsettings get org.gnome.login-screen disable-user-list

true
```

If the setting is "false", this is a finding.

Internal Only - General

Remediation:

Configure the operating system to disable the user list at logon for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/02-login-screen
[org/gnome/login-screen]
disable-user-list=true
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.158 OL08-00-020035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must terminate idle user sessions.

```
GROUP ID: V-257259
RULE ID: SV-257259r970703
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended.

Audit:

Verify that OL 8 logs out sessions that are idle for 15 minutes with the following command:

```
 $ sudo grep -i ^StopIdleSessionSec /etc/systemd/logind.conf

 StopIdleSessionSec=900
```

If "StopIdleSessionSec" is not configured to 900 seconds, this is a finding.

Remediation:

Configure OL 8 to log out idle sessions by editing the /etc/systemd/logind.conf file with the following line:

```
 StopIdleSessionSec=900
```

The "logind" service must be restarted for the changes to take effect. To restart the "logind" service, run the following command:

```
 $ sudo systemctl restart systemd-logind
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

Internal Only - General

1.159 OL08-00-020043 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable a user session lock until that user reestablishes access using established identification and authentication procedures for command line sessions.

```
GROUP ID: V-248678
RULE ID: SV-248678r1015045
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, OL 8 needs to provide users with the ability to manually invoke a session lock so users may secure their session should the need arise for them to temporarily vacate the immediate physical vicinity.

Systemd, a core component of OL 8, has a variety of dependencies needed to function. One of those packages is the Keytable files and keyboard utilities (kbd.x86_64). This package provides the "vlock" binary, a utility used to lock one or several user virtual console sessions.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify OL 8 has the "vlock" package installed by running the following command:

```
$ sudo grep vlock /usr/bin/*

Binary file /usr/bin/vlock matches
```

If "vlock" is not installed, this is a finding.

Remediation:

Install the "vlock" package, if it is not already installed, by running the following command:

```
$ sudo yum install kbd.x86_64
```


Internal Only - General

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

Internal Only - General

1.160 OL08-00-020050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be able to initiate directly a session lock for all connection types using smartcard when the smartcard is removed.

```
GROUP ID: V-248679
RULE ID: SV-248679r1015046
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

OL 8 includes "authselect" as a tool to configure system identity, authentication sources, and providers by selecting a specific profile. A profile is a set of files that describes the resulting system configuration. When a profile is selected, "authselect" will create the "nsswitch.conf" and "PAM" stack to use identity and authentication sources defined by the profile.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system enables a user's session lock until that user reestablishes access using established identification and authentication procedures with the following command:

This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ sudo grep -r removal-action /etc/dconf/db/*

/etc/dconf/db/distro.d/20-authselect:removal-action='lock-screen'
```

If the "removal-action='lock-screen'" setting is missing or commented out from the "dconf" database files, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to enable a user's session lock until that user reestablishes access using established identification and authentication procedures.

Select/create an "authselect" profile and incorporate the "with-smartcard-lock-on-removal" feature as in the following example:

```
$ sudo authselect select sssd with-smartcard with-smartcard-lock-on-removal
```

Alternatively, the "dconf" settings can be edited in the "/etc/dconf/db/*" location.

Edit or add the "[org/gnome/settings-daemon/peripherals/smartcard]" section of the database file and add or update the following line:

```
removal-action='lock-screen'
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

Internal Only - General

1.161 OL08-00-020060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must automatically lock graphical user sessions after 15 minutes of inactivity.

```
GROUP ID: V-248680
RULE ID: SV-248680r958402
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems must be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces with the following commands:

```
$ sudo gsettings get org.gnome.desktop.session idle-delay

uint32 900
```

If "idle-delay" is set to "0" or a value greater than "900", this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
$ sudo touch /etc/dconf/db/local.d/00-screensaver
```

Edit "/etc/dconf/db/local.d/00-screensaver" and add or update the following lines:

```
[org/gnome/desktop/session]
# Set the lock time out to 900 seconds before the session is considered idle
idle-delay=uint32 900
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.162 OL08-00-020080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent a user from overriding the session lock-delay setting for the graphical user interface.

```
GROUP ID: V-248682
RULE ID: SV-248682r958402
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Internal Only - General

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system prevents a user from overriding settings for graphical user interfaces.

Determine which profile the system database is using with the following command:

```
$ sudo grep system-db /etc/dconf/profile/user

system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command.

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
$ sudo grep -i lock-delay /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/lock-delay
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure OL 8 to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command.

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/screensaver/lock-delay
```


Internal Only - General

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.163 OL08-00-020081 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent a user from overriding the session idle-delay setting for the graphical user interface.

```
GROUP ID: V-248683
RULE ID: SV-248683r958402
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Internal Only - General

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system prevents a user from overriding settings for graphical user interfaces.

Determine which profile the system database is using with the following command:

```
$ sudo grep system-db /etc/dconf/profile/user

system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command.

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
$ sudo grep -i idle /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/idle-delay
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure OL 8 to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command.

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/screensaver/idle-delay
```


Internal Only - General

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.164 OL08-00-020082 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent a user from overriding the session lock-enabled setting for the graphical user interface.

```
GROUP ID: V-248684
RULE ID: SV-248684r958402
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Internal Only - General

Audit:

Note: This requirement assumes the use of the OL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Verify the operating system prevents a user from overriding settings for graphical user interfaces.

Determine which profile the system database is using with the following command:

```
$ sudo grep system-db /etc/dconf/profile/user

system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command.

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
$ sudo grep -i lock-enabled /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/lock-enabled
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure OL 8 to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command.

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/screensaver/lock-enabled
```


Internal Only - General

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

Internal Only - General

1.165 OL08-00-020090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must map the authenticated identity to the user or group account for PKI-based authentication.

```
GROUP ID: V-248685
RULE ID: SV-248685r958452
```

Rationale:

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

There are various methods of mapping certificates to user/group accounts for OL 8. For the purposes of this requirement, the check and fix will account for Active Directory mapping. Some of the other possible methods include joining the system to a domain and using an idM server, or a local system mapping, where the system is not part of a domain.

Audit:

Verify the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file with the following command:

Note: If the System Administrator demonstrates the use of an approved alternate multifactor authentication method, this requirement is not applicable.

```
$ sudo cat /etc/sssd/sssd.conf

[sssd]
config_file_version = 2
services = pam, sudo, ssh
domains = testing.test

[pam]
pam_cert_auth = True

[domain/testing.test]
id_provider = ldap

[certmap/testing.test/rule_name]
matchrule =<SAN>.*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

If the "certmap" section does not exist, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to map the authenticated identity to the user or group account by adding or modifying the "certmap" section of the "/etc/sssd/sssd.conf" file based on the following example:

```
[certmap/testing.test/rule_name]
matchrule =<SAN>.*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (c)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (2)

Internal Only - General

1.166 OL08-00-020100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must ensure the password complexity module is enabled in the password-auth file.

```
GROUP ID: V-248686
RULE ID: SV-248686r982195
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Use of "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. This is set in both of the following: /etc/pam.d/password-auth /etc/pam.d/system-auth

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038

Audit:

Verify the operating system uses "pwquality" to enforce the password complexity rules.

Check for the use of "pwquality" in the password-auth file with the following command:

```
 $ sudo cat /etc/pam.d/password-auth | grep pam_pwquality

 password requisite pam_pwquality.so
```

If the command does not return a line containing the value "pam_pwquality.so" as shown, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to use "pwquality" to enforce password complexity rules.

Add the following line to the "/etc/pam.d/password-auth" file (or modify the line to have the required value):

```
 password requisite pam_pwquality.so
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.167 OL08-00-020101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must ensure the password complexity module is enabled in the system-auth file.

```
GROUP ID: V-252657
RULE ID: SV-252657r991589
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

OL 8 utilizes "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth

Audit:

Verify the operating system uses "pwquality" to enforce the password complexity rules.

Check for the use of "pwquality" in the system-auth file with the following command:

```
 $ sudo cat /etc/pam.d/system-auth | grep pam_pwquality

 password requisite pam_pwquality.so
```

If the command does not return a line containing the value "pam_pwquality.so" as shown, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to use "pwquality" to enforce password complexity rules.

Add the following line to the "/etc/pam.d/system-auth" file (or modify the line to have the required value):

```
 password requisite pam_pwquality.so
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.168 OL08-00-020102 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.4 must ensure the password complexity module in the system-auth file is configured for three retries or less.

```
GROUP ID: V-252658
RULE ID: SV-252658r991589
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

OL 8 utilizes "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

Audit:

Note: This requirement applies to OL versions 8.0 through 8.3. If the system is OL version 8.4 or newer, this requirement is not applicable.

Verify the operating system is configured to limit the "pwquality" retry option to 3.

Check for the use of the "pwquality" retry option in the system-auth file with the following command:

```
 $ sudo cat /etc/pam.d/system-auth | grep pam_pwquality

 password requisite pam_pwquality.so retry=3
```

If the value of "retry" is set to "0" or greater than "3", this is a finding.

Remediation:

Configure the operating system to limit the "pwquality" retry option to 3.

Add the following line to the "/etc/pam.d/system-auth" file (or modify the line to have the required value):

```
 password requisite pam_pwquality.so retry=3
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.169 OL08-00-020103 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems below version 8.4 must ensure the password complexity module in the password-auth file is configured for three retries or less.

```
GROUP ID: V-252659
RULE ID: SV-252659r991589
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

OL 8 utilizes "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

Audit:

Note: This requirement applies to OL versions 8.0 through 8.3. If the system is OL version 8.4 or newer, this requirement is not applicable.

Verify the operating system is configured to limit the "pwquality" retry option to 3.

Check for the use of the "pwquality" retry option in the password-auth file with the following command:

```
$ sudo cat /etc/pam.d/password-auth | grep pam_pwquality

password requisite pam_pwquality.so retry=3
```

If the value of "retry" is set to "0" or greater than "3", this is a finding.

Remediation:

Configure the operating system to limit the "pwquality" retry option to 3.

Add the following line to the "/etc/pam.d/password-auth" file (or modify the line to have the required value):

```
password requisite pam_pwquality.so retry=3
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.170 OL08-00-020104 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 systems, version 8.4 and above, must ensure the password complexity module is configured for three retries or less.

```
GROUP ID: V-252660
RULE ID: SV-252660r991589
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

OL 8 utilizes "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

Audit:

Note: This requirement applies to OL versions 8.4 or newer. If the system is OL below version 8.4, this requirement is not applicable.

Verify the operating system is configured to limit the "pwquality" retry option to 3.

Check for the use of the "pwquality" retry option with the following command:

```
$ sudo grep -r retry /etc/security/pwquality.conf*

/etc/security/pwquality.conf:retry = 3
```

If the value of "retry" is set to "0" or greater than "3", is commented out or missing, this is a finding.

If conflicting results are returned, this is a finding.

Check for the use of the "pwquality" retry option in the system-auth and password-auth files with the following command:

```
$ sudo grep pwquality /etc/pam.d/system-auth /etc/pam.d/password-auth | grep
retry
```

If the command returns any results, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to limit the "pwquality" retry option to 3.

Add the following line to the "/etc/security/pwquality.conf" file(or modify the line to have the required value):

```
retry = 3
```

Remove any configurations that conflict with the above value.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.171 OL08-00-020110 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-248687
RULE ID: SV-248687r1015047
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses pwquality as a mechanism to enforce password complexity. Note that in order to require uppercase characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038

Audit:

Verify the value for "ucredit" in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r ucredit /etc/security/pwquality.conf*

/etc/security/pwquality.conf:ucredit = -1
```

If the value of "ucredit" is a positive number or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to enforce password complexity by requiring that at least one uppercase character be used by setting the "ucredit" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
ucredit = -1
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

Internal Only - General

1.172 OL08-00-020120 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must enforce password complexity by requiring that at least one lowercase character be used.

```
GROUP ID: V-248688
RULE ID: SV-248688r1015048
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses pwquality as a mechanism to enforce password complexity. Note that in order to require lowercase characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "lcredit" in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r lcredit /etc/security/pwquality.conf*

/etc/security/pwquality.conf:lcredit = -1
```

If the value of "lcredit" is a positive number or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to enforce password complexity by requiring that at least one lowercase character be used by setting the "lcredit" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
lcredit = -1
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

Internal Only - General

1.173 OL08-00-020130 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-248689
RULE ID: SV-248689r1015049
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. Note that in order to require numeric characters without degrading the minlen value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "dcredit" in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r dcredit /etc/security/pwquality.conf*

/etc/security/pwquality.conf:dcredit = -1
```

If the value of "dcredit" is a positive number or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to enforce password complexity by requiring that at least one numeric character be used by setting the "dcredit" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
dcredit = -1
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

Internal Only - General

1.174 OL08-00-020140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.

```
GROUP ID: V-248690
RULE ID: SV-248690r1015050
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. The "maxclassrepeat" option sets the maximum number of allowed same consecutive characters in the same class in the new password.

Audit:

Check for the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r maxclassrepeat /etc/security/pwquality.conf*

/etc/security/pwquality.conf:maxclassrepeat = 4
```

If the value of "maxclassrepeat" is set to "0", more than "4" or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
maxclassrepeat = 4
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53::IA-5 (1) (b)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (b)

Internal Only - General

1.175 OL08-00-020150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must require the maximum number of repeating characters be limited to three when passwords are changed.

```
GROUP ID: V-248691
RULE ID: SV-248691r1015051
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. The "maxrepeat" option sets the maximum number of allowed same consecutive characters in a new password.

Audit:

Check for the value of the "maxrepeat" option in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r maxrepeat /etc/security/pwquality.conf*

/etc/security/pwquality.conf:maxrepeat = 3
```

If the value of "maxrepeat" is set to more than "3" or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to require the change of the number of repeating consecutive characters when passwords are changed by setting the "maxrepeat" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
maxrepeat = 3
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53::IA-5 (1) (b)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (b)

Internal Only - General

1.176 OL08-00-020160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must require the change of at least four character classes when passwords are changed.

```
GROUP ID: V-248692
RULE ID: SV-248692r1015052
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. The "minclass" option sets the minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others).

Audit:

Verify the value of the "minclass" option in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r minclass /etc/security/pwquality.conf*

/etc/security/pwquality.conf:minclass = 4
```

If the value of "minclass" is set to less than "4" or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to require the change of at least four character classes when passwords are changed by setting the "minclass" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
minclass = 4
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53::IA-5 (1) (b)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (b)

Internal Only - General

1.177 OL08-00-020170 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must require the change of at least eight characters when passwords are changed.

```
GROUP ID: V-248693
RULE ID: SV-248693r1015053
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. The "difok" option sets the number of characters in a password that must not be present in the old password.

Audit:

Verify the value of the "difok" option in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r difok /etc/security/pwquality.conf*

/etc/security/pwquality.conf:difok = 8
```

If the value of "difok" is set to less than "8" or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to require the change of at least eight of the total number of characters when passwords are changed by setting the "difok" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
difok = 8
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53::IA-5 (1) (b)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (b)

Internal Only - General

1.178 OL08-00-020180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 passwords for new users or password changes must have a 24 hours/one day minimum password lifetime restriction in "/etc/shadow".

```
GROUP ID: V-248694
RULE ID: SV-248694r1015054
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Verify the minimum time period between password changes for each user account is one day or greater.

```
$ sudo awk -F: '$4 < 1 {print $1 " " $4}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure non-compliant accounts to enforce a 24 hours/one day minimum password lifetime:

```
$ sudo chage -m 1 [user]
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

Internal Only - General

1.179 OL08-00-020190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 passwords for new users or password changes must have a 24 hours/one day minimum password lifetime restriction in "/etc/login.defs".

```
GROUP ID: V-248695
RULE ID: SV-248695r1015055
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Verify the operating system enforces 24 hours/one day as the minimum password lifetime for new user accounts.

Check for the value of "PASS_MIN_DAYS" in "/etc/login.defs" with the following command:

```
$ sudo grep -i pass_min_days /etc/login.defs

PASS_MIN_DAYS 1
```

If the "PASS_MIN_DAYS" parameter value is not "1" or greater or is commented out, this is a finding.

Remediation:

Configure OL 8 to enforce 24 hours/one day as the minimum password lifetime.

Add the following line in "/etc/login.defs" (or modify the line to have the required value):

```
PASS_MIN_DAYS 1
```


Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

Internal Only - General

1.180 OL08-00-020200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 user account passwords must have a 60-day maximum password lifetime restriction.

```
GROUP ID: V-248696
RULE ID: SV-248696r1038967
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If OL 8 does not limit the lifetime of passwords and force users to change their passwords, there is the risk that OL 8 passwords could be compromised.

Audit:

Verify that OL 8 enforces a 60-day maximum password lifetime for new user accounts by running the following command:

```
$ sudo grep -i pass_max_days /etc/login.defs

PASS_MAX_DAYS 60
```

If the "PASS_MAX_DAYS" parameter value is greater than "60", or commented out, this is a finding.

Remediation:

Configure OL 8 to enforce a 60-day maximum password lifetime.

Add or modify the following line in the "/etc/login.defs" file:

```
PASS_MAX_DAYS 60
```


Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

Internal Only - General

1.181 OL08-00-020210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 user account passwords must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

```
GROUP ID: V-248697
RULE ID: SV-248697r1038967
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If OL 8 does not limit the lifetime of passwords and force users to change their passwords, there is the risk that OL 8 passwords could be compromised.

Audit:

Verify the maximum time period for existing passwords is restricted to 60 days with the following commands:

```
$ sudo awk -F: '$5 > 60 {print $1 " " $5}' /etc/shadow
$ sudo awk -F: '$5 <= 0 {print $1 " " $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.

```
$ sudo chage -M 60 [user]
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

Internal Only - General

1.182 OL08-00-020230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 passwords must have a minimum of 15 characters.

```
GROUP ID: V-248699
RULE ID: SV-248699r1015058
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. Configurations are set in the "etc/security/pwquality.conf" file.

The "minlen", sometimes noted as minimum length, acts as a "score" of complexity based on the credit components of the "pwquality" module. By setting the credit components to a negative value, not only will those components be required, but they will not count toward the total "score" of "minlen". This will enable "minlen" to require a 15-character minimum.

Audit:

Verify the operating system enforces a minimum 15-character password length. The "minlen" option sets the minimum number of characters in a new password.

Check for the value of the "minlen" option in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r minlen /etc/security/pwquality.conf*

/etc/security/pwquality.conf:minlen = 15
```

If the command does not return a "minlen" value of 15 or greater or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to enforce a minimum 15-character password length.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
minlen = 15
```

Remove any configurations that conflict with the above value.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (i)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

Internal Only - General

1.183 OL08-00-020231 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 passwords for new users must have a minimum of 15 characters.

```
GROUP ID: V-248700
RULE ID: SV-248700r1015059
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

The DOD minimum password requirement is 15 characters.

Audit:

Verify that OL 8 enforces a minimum 15-character password length for new user accounts by running the following command:

```
$ sudo grep -i pass_min_len /etc/login.defs

PASS_MIN_LEN 15
```

If the "PASS_MIN_LEN" parameter value is less than "15" or is commented out, this is a finding.

Remediation:

Configure operating system to enforce a minimum 15-character password length for new user accounts.

Add or modify the following line in the "/etc/login.defs" file:

```
PASS_MIN_LEN 15
```


Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (i)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

Internal Only - General

1.184 OL08-00-020240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 duplicate User IDs (UIDs) must not exist for interactive users.

```
GROUP ID: V-248701
RULE ID: SV-248701r958422
```

Rationale:

To ensure accountability and prevent unauthenticated access, interactive users must be identified and authenticated to prevent potential misuse and compromise of the system.

Interactive users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Interactive users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1. Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and
2. Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000104-GPOS-00051, SRG-OS-000121-GPOS-00062

Audit:

Verify that OL 8 contains no duplicate UIDs for interactive users with the following command:

```
$ sudo awk -F ":" 'list[$3]++{print $1, $3}' /etc/passwd
```

If output is produced and the accounts listed are interactive user accounts, this is a finding.

Remediation:

Edit the file "/etc/passwd" and provide each interactive user account that has a duplicate UID with a unique UID.

Internal Only - General

Additional Information:

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8
- NIST SP 800-53 Revision 5::IA-8

Internal Only - General

1.185 OL08-00-020250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must implement multifactor authentication for access to interactive accounts.

```
GROUP ID: V-248702
RULE ID: SV-248702r1015060
```

Rationale:

Using an authentication device, such as a Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DOD CAC.

There are various methods of implementing multifactor authentication for OL 8. Some methods include a local system multifactor account mapping or joining the system to a domain and using an idM server or Microsoft Windows Active Directory server. Any of these methods will require that the client operating system handle the multifactor authentication correctly.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Internal Only - General

Audit:

Verify OL 8 uses multifactor authentication for local access to accounts.

Note: If the system administrator (SA) demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.

Check that the "pam_cert_auth" setting is set to "true" in the "/etc/sssd/sssd.conf" file.

Check that the "try_cert_auth" or "require_cert_auth" options are configured in both "/etc/pam.d/system-auth" and "/etc/pam.d/smartcard-auth" files with the following command:

```
$ sudo grep -ir cert_auth /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
/etc/pam.d/*

/etc/sssd/sssd.conf:pam_cert_auth = True
/etc/pam.d/smartcard-auth:auth sufficient pam_sss.so try_cert_auth
/etc/pam.d/system-auth:auth [success=done authinfo_unavail=ignore
ignore=ignore default=die] pam_sss.so try_cert_auth
```

If "pam_cert_auth" is not set to "true" in "/etc/sssd/sssd.conf", this is a finding.

If "pam_sss.so" is not set to "try_cert_auth" or "require_cert_auth" in both the "/etc/pam.d/smartcard-auth" and "/etc/pam.d/system-auth" files, this is a finding.

Remediation:

Configure OL 8 to use multifactor authentication for local access to accounts.

Add or update the "pam_cert_auth" setting in the "/etc/sssd/sssd.conf" file to match the following line:

```
 [pam]
 pam_cert_auth = True
```

Add or update "pam_sss.so" with "try_cert_auth" or "require_cert_auth" in the "/etc/pam.d/system-auth" and "/etc/pam.d/smartcard-auth" files based on the following examples:

```
 /etc/pam.d/smartcard-auth:auth sufficient pam_sss.so try_cert_auth

 /etc/pam.d/system-auth:auth [success=done authinfo_unavail=ignore
ignore=ignore default=die] pam_sss.so try_cert_auth
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
 $ sudo systemctl restart sssd.service
```


Internal Only - General

Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

Internal Only - General

1.186 OL08-00-020260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 system-auth file must disable access to the system for account identifiers (individuals, groups, roles, and devices) with 35 days of inactivity.

```
GROUP ID: V-248703
RULE ID: SV-248703r1015061
```

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

OL 8 needs to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Audit:

Verify the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity by checking the account inactivity value with the following command:

```
$ sudo grep 'inactive\|pam_unix' /etc/pam.d/system-auth | grep -w auth

auth      required      pam_lastlog.so inactive=35
auth      sufficient     pam_unix.so
```

If the pam_lastlog.so module is listed below the pam_unix.so module in the "system-auth" file, this is a finding.

If the value of "inactive" is set to zero, a negative number, or is greater than 35, this is a finding.

If the line is commented out or missing, ask the administrator to indicate how the system disables access for account identifiers. If there is no evidence that the system is disabling access for account identifiers after 35 days of inactivity, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable access to the system for account identifiers with 35 days of inactivity.

Add/Modify the following line to "/etc/pam.d/system-auth" above the "pam_unix.so" statement:

```
auth      required      pam_lastlog.so inactive=35
```

Note: The DOD recommendation is 35 days, but a lower value is acceptable.

Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5::AC-2 (3) (b)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

Internal Only - General

1.187 OL08-00-020261 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 password-auth file must disable access to the system for account identifiers (individuals, groups, roles, and devices) with 35 days of inactivity.

```
GROUP ID: V-248704
RULE ID: SV-248704r1015062
```

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

OL 8 needs to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Audit:

Verify the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity by checking the account inactivity value with the following command:

```
$ sudo grep 'inactive\|pam_unix' /etc/pam.d/password-auth | grep -w auth

auth      required      pam_lastlog.so inactive=35
auth      sufficient     pam_unix.so
```

If the pam_lastlog.so module is listed below the pam_unix.so module in the "password-auth" file, this is a finding.

If the value of "inactive" is set to zero, a negative number, or is greater than 35, this is a finding.

If the line is commented out or missing, ask the administrator to indicate how the system disables access for account identifiers. If there is no evidence that the system is disabling access for account identifiers after 35 days of inactivity, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable access to the system for account identifiers with 35 days of inactivity.

Add/Modify the following line to "/etc/pam.d/password-auth" above the "pam_unix.so" statement:

```
auth      required      pam_lastlog.so inactive=35
```

Note: The DOD recommendation is 35 days, but a lower value is acceptable.

Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5::AC-2 (3) (b)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

Internal Only - General

1.188 OL08-00-020262 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 lastlog command must have a mode of "0750" or less permissive.

```
GROUP ID: V-248705
RULE ID: SV-248705r958566
```

Rationale:

Unauthorized disclosure of the contents of the /var/log/lastlog file can reveal system data to attackers, thus compromising its confidentiality.

Audit:

Verify the "lastlog" command has a mode of "0750" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /usr/bin/lastlog

750  /usr/bin/lastlog
```

If the "lastlog" command has a mode more permissive than "0750", this is a finding.

Remediation:

Configure the mode of the "lastlog" command for OL 8 to "0750" with the following command:

```
$ sudo chmod 0750 /usr/bin/lastlog
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.189 OL08-00-020263 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 lastlog command must be owned by root.

```
GROUP ID: V-248706
RULE ID: SV-248706r958566
```

Rationale:

Unauthorized disclosure of the contents of the /var/log/lastlog file can reveal system data to attackers, thus compromising its confidentiality.

Audit:

Verify the "lastlog" command is owned by root with the following command:

```
$ sudo ls -l /usr/bin/lastlog

-rwxr-x---. 1  root  root  21200 Nov  4   22:51  /usr/bin/lastlog
```

If the "lastlog" command is not owned by root, this is a finding.

Remediation:

Configure the "lastlog" command for OL 8 to be owned by root with the following command:

```
$ sudo chown root /usr/bin/lastlog
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.190 OL08-00-020264 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 lastlog command must be group-owned by root.

```
GROUP ID: V-248707
RULE ID: SV-248707r958566
```

Rationale:

Unauthorized disclosure of the contents of the /var/log/lastlog file can reveal system data to attackers, thus compromising its confidentiality.

Audit:

Verify the "lastlog" command is group-owned by root with the following command:

```
$ sudo ls -l /usr/bin/lastlog

-rwxr-x---. 1  root  root  21200 Nov  4   22:51  /usr/bin/lastlog
```

If the "lastlog" command is not group-owned by root, this is a finding.

Remediation:

Configure the "lastlog" command for OL 8 to be group-owned by root with the following command:

```
$ sudo chgrp root /usr/bin/lastlog
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Internal Only - General

1.191 OL08-00-020270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must automatically expire temporary accounts within 72 hours.

```
GROUP ID: V-248708
RULE ID: SV-248708r958508
```

Rationale:

Temporary accounts are privileged or nonprivileged accounts that are established during pressing circumstances, such as new software or hardware configuration or an incident response, where the need for prompt account activation requires bypassing normal account authorization procedures. If any inactive temporary accounts are left enabled on the system and are not either manually removed or automatically expired within 72 hours, the security posture of the system will be degraded and exposed to expoitation by unauthorized users or insider threat actors.

Temporary accounts are different from emergency accounts. Emergency accounts, also known as "last resort" or "break glass" accounts, are local logon accounts enabled on the system for emergency use by authorized system administrators to manage a system when standard logon methods are failing or not available. Emergency accounts are not subject to manual removal or scheduled expiration requirements.

The automatic expiration of temporary accounts may be extended as needed by the circumstances but it must not be extended indefinitely. A documented permanent account should be established for privileged users who need long-term maintenance accounts.

Audit:

Verify temporary accounts have been provisioned with an expiration date of 72 hours.

For every existing temporary account, run the following command to obtain its account expiration information:

```
 $ sudo chage -l <temporary_account_name> | grep -i "account expires"
```

Verify each of these accounts has an expiration date set within 72 hours.

If any temporary accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to expire temporary accounts after 72 hours with the following command:

```
$ sudo chage -E $(date -d +3days +%Y-%m-%d) <temporary_account_name>
```

Additional Information:

CCI-001682 Automatically remove or disable emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 Revision 5::AC-2 (2)
- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)

Internal Only - General

1.192 OL08-00-020280 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

All OL 8 passwords must contain at least one special character.

```
GROUP ID: V-248709
RULE ID: SV-248709r1015063
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

OL 8 uses "pwquality" as a mechanism to enforce password complexity. Note that to require special characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify the value for "ocredit" in "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r ocredit /etc/security/pwquality.conf*

/etc/security/pwquality.conf:ocredit = -1
```

If the value of "ocredit" is a positive number or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to enforce password complexity by requiring that at least one special character be used by setting the "ocredit" option.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
ocredit = -1
```

Remove any configurations that conflict with the above value.

Internal Only - General

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

Internal Only - General

1.193 OL08-00-020290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prohibit the use of cached authentications after one day.

```
GROUP ID: V-248710
RULE ID: SV-248710r958828
```

Rationale:

If cached authentication information is out of date, the validity of the authentication information may be questionable.

OL 8 includes multiple options for configuring authentication, but this requirement will focus on the System Security Services Daemon (SSSD). By default, SSSD does not cache credentials.

Audit:

Verify that the SSSD prohibits the use of cached authentications after one day.

Note: If smart card authentication is not being used on the system, this item is not applicable.

Check that SSSD allows cached authentications with the following command:

```
 $ sudo grep -ir cache_credentials /etc/sssd/sssd.conf
/etc/sssd/conf.d/*.conf

 cache_credentials = true
```

If "cache_credentials" is set to "false" or is missing from the configuration file, this is not a finding and no further checks are required.

If "cache_credentials" is set to "true", check that SSSD prohibits the use of cached authentications after one day with the following command:

```
 $ sudo grep -ir offline_credentials_expiration /etc/sssd/sssd.conf
/etc/sssd/conf.d/*.conf

 offline_credentials_expiration = 1
```

If "offline_credentials_expiration" is not set to a value of "1", this is a finding.

Internal Only - General

Remediation:

Configure the SSSD to prohibit the use of cached authentications after one day.

Add or change the following line in "/etc/sssd/sssd.conf" just below the line "[pam]".

```
offline_credentials_expiration = 1
```

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

Internal Only - General

1.194 OL08-00-020300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent the use of dictionary words for passwords.

```
GROUP ID: V-248711
RULE ID: SV-248711r991587
```

Rationale:

If OL 8 allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

Audit:

Verify OL 8 prevents the use of dictionary words for passwords.

Determine if the field "dictcheck" is set in the "/etc/security/pwquality.conf" or "/etc/security/pwquality.conf.d/*.conf" files with the following command:

```
$ sudo grep -r dictcheck /etc/security/pwquality.conf*

/etc/security/pwquality.conf:dictcheck=1
```

If the "dictcheck" parameter is not set to "1" or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to prevent the use of dictionary words for passwords.

Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory:

```
dictcheck=1
```

Remove any configurations that conflict with the above value.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.195 OL08-00-020310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-248712
RULE ID: SV-248712r991588
```

Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt with the following command:

```
$ sudo grep -i fail_delay /etc/login.defs

FAIL_DELAY 4
```

If the value of "FAIL_DELAY" is not set to "4" or greater or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.

Modify the "/etc/login.defs" file to set the "FAIL_DELAY" parameter to "4" or greater:

```
FAIL_DELAY 4
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.196 OL08-00-020320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have unnecessary accounts.

```
GROUP ID: V-248713
RULE ID: SV-248713r991589
```

Rationale:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Audit:

Verify all accounts on the system are assigned to an active system, application, or user account.

Obtain the list of authorized system accounts from the Information System Security Officer (ISSO).

Check the system accounts on the system with the following command:

```
$ sudo more /etc/passwd

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
```

Accounts such as "games" and "gopher" are not authorized accounts as they do not support authorized system functions.

If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding.

Internal Only - General

Remediation:

Configure the system so all accounts on the system are assigned to an active system, application, or user account.

Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.

Document all authorized accounts on the system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.197 OL08-00-020330 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must not allow accounts configured with blank or null passwords.

```
GROUP ID: V-248714
RULE ID: SV-248714r991589
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*permitemptypasswords'

PermitEmptyPasswords no
```

If "PermitEmptyPasswords" is set to "yes", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Edit the following line in "etc/ssh/sshd_config" to prevent logons with empty passwords.

PermitEmptyPasswords no

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.198 OL08-00-020331 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must not allow blank or null passwords in the system-auth file.

```
GROUP ID: V-248715
RULE ID: SV-248715r991589
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
$ sudo grep -i nullok /etc/pam.d/system-auth
```

If output is produced, this is a finding.

Remediation:

Remove any instances of the "nullok" option in the "/etc/pam.d/system-auth" file to prevent logons with empty passwords.

Note: Manual changes to the listed file may be overwritten by the "authselect" program.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.199 OL08-00-020332 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must not allow blank or null passwords in the password-auth file.

```
GROUP ID: V-248716
RULE ID: SV-248716r991589
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
$ sudo grep -i nullok /etc/pam.d/password-auth
```

If output is produced, this is a finding.

Remediation:

Remove any instances of the "nullok" option in the "/etc/pam.d/password-auth" file to prevent logons with empty passwords.

Note: Manual changes to the listed file may be overwritten by the "authselect" program.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.200 OL08-00-020340 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must display the date and time of the last successful account logon upon logon.

```
GROUP ID: V-248717
RULE ID: SV-248717r991589
```

Rationale:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify users are provided with feedback on when account accesses last occurred with the following command:

```
$ sudo grep pam_lastlog /etc/pam.d/postlogin

session required pam_lastlog.so showfailed
```

If "pam_lastlog" is missing from the "/etc/pam.d/postlogin" file or the silent option is present, this is a finding.

Remediation:

Configure OL 8 to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin".

Add the following line to the top of "/etc/pam.d/postlogin":

```
session required pam_lastlog.so showfailed
```

Additional Information:

CCI-000052 Notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

- NIST SP 800-53::AC-9
- NIST SP 800-53A::AC-9.1
- NIST SP 800-53 Revision 4::AC-9
- NIST SP 800-53 Revision 5::AC-9

Internal Only - General

1.201 OL08-00-020350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must display the date and time of the last successful account logon upon an SSH logon.

```
GROUP ID: V-248718
RULE ID: SV-248718r991589
```

Rationale:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify SSH provides users with feedback on when account accesses last occurred with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*printlastlog'

PrintLastLog yes
```

If the "PrintLastLog" keyword is set to "no", is missing, or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/sshd" or in the "sshd_config" file used by the system ("/etc/ssh/sshd_config" will be used in the example). Note that this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor.

Modify the "PrintLastLog" line in "/etc/ssh/sshd_config" to match the following:

```
PrintLastLog yes
```

The SSH service must be restarted for changes to "sshd_config" to take effect.

Internal Only - General

Additional Information:

CCI-000052 Notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

- NIST SP 800-53::AC-9
- NIST SP 800-53A::AC-9.1
- NIST SP 800-53 Revision 4::AC-9
- NIST SP 800-53 Revision 5::AC-9

Internal Only - General

1.202 OL08-00-020351 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 default permissions must be defined in such a way that all authenticated users can read and modify only their own files.

```
GROUP ID: V-248719
RULE ID: SV-248719r991590
```

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Audit:

Verify OL 8 defines default permissions for all authenticated users in such a way that the user can read and modify only their own files with the following command:

```
$ sudo grep -i "umask" /etc/login.defs

UMASK 077
```

If the "UMASK" variable is set to "000", this is a finding with the severity raised to a CAT I.

If the value of "UMASK" is not set to "077", "UMASK" is commented out, or "UMASK" is missing completely, this is a finding.

Remediation:

Configure OL 8 to define the default permissions for all authenticated users in such a way that the user can read and modify only their own files.

Edit the "UMASK" parameter in the "/etc/login.defs" file to match the example below:

```
UMASK 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.203 OL08-00-020352 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must set the umask value to 077 for all local interactive user accounts.

```
GROUP ID: V-248720
RULE ID: SV-248720r991590
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the default umask for all local interactive users is "077".

Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.

Check all local interactive user initialization files for interactive users with the following command:

Note: The example is for a system that is configured to create users home directories in the "/home" directory.

```
$ sudo grep -ir ^umask /home | grep -v '.bash_history'
```

If any local interactive user initialization files are found to have a umask statement that has a value less restrictive than "077", this is a finding.

Remediation:

Remove the umask statement from all local interactive user's initialization files.

If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the Information System Security Officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.204 OL08-00-020353 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must define default permissions for logon and non-logon shells.

```
GROUP ID: V-248721
RULE ID: SV-248721r991590
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the umask default for installed shells is "077".

Check for the value of the "UMASK" parameter in the "/etc/bashrc", "/etc/csh.cshrc", and "/etc/profile" files with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in the "/etc/bashrc", "/etc/csh.cshrc", or the "/etc/profile" files, the Severity is raised to a CAT I.

```
$ sudo  grep -i umask /etc/bashrc /etc/csh.cshrc /etc/profile

/etc/bashrc: umask 077
/etc/bashrc: umask 077
/etc/csh.cshrc: umask 077
/etc/csh.cshrc: umask 077
/etc/profile: umask 077
/etc/profile: umask 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the lines for the "UMASK" parameter in the "/etc/bashrc", "etc/csh.cshrc", and "/etc/profile" files to "077":

```
UMASK 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.205 OL08-00-030000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit system must be configured to audit the execution of privileged functions and prevent all software from executing at higher privilege levels than users executing the software.

```
GROUP ID: V-248722
RULE ID: SV-248722r958730
```

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

Audit:

Verify OL 8 audits the execution of privileged functions.

Check if OL 8 is configured to audit the execution of the "execve" system call, by running the following command:

```
$ sudo grep execve /etc/audit/audit.rules

-a always,exit -F arch=b32 -S execve -C uid!=euid -F key=execpriv
-a always,exit -F arch=b64 -S execve -C uid!=euid -F key=execpriv

-a always,exit -F arch=b32 -S execve -C gid!=egid -F key=execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F key=execpriv
```

If the command does not return all lines or the lines are commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to audit the execution of the "execve" system call.

Add or update the following file system rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F key=execpriv
-a always,exit -F arch=b64 -S execve -C uid!=euid -F key=execpriv

-a always,exit -F arch=b32 -S execve -C gid!=egid -F key=execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F key=execpriv
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-002233 Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4::AC-6 (8)
- NIST SP 800-53 Revision 5::AC-6 (8)

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)
- NIST SP 800-53 Revision 5::AC-6 (9)

Internal Only - General

1.206 OL08-00-030010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Cron logging must be implemented in OL 8.

```
GROUP ID: V-248723
RULE ID: SV-248723r991589
```

Rationale:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Audit:

Verify that "rsyslog" is configured to log cron events with the following command:

Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files.

```
$ sudo grep cron /etc/rsyslog.conf /etc/rsyslog.d/*.conf

cron.* /var/log/cron
```

If the command does not return a response, check for cron logging all facilities by inspecting the "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files.

Look for the following entry:

```
*.* /var/log/messages
```

If "rsyslog" is not logging messages for the cron facility or all facilities, this is a finding.

Remediation:

Configure "rsyslog" to log all cron messages by adding or updating the following line to "/etc/rsyslog.conf" or a configuration file in the "/etc/rsyslog.d/" directory:

```
cron.* /var/log/cron
```

The rsyslog daemon must be restarted for the changes to take effect:

```
$ sudo systemctl restart rsyslog.service
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.207 OL08-00-030020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.

```
GROUP ID: V-248724
RULE ID: SV-248724r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify that the SA and ISSO (at a minimum) are notified in the event of an audit processing failure with the following command:

```
$ sudo grep action_mail_acct /etc/audit/auditd.conf

action_mail_acct = root
```

If the value of the "action_mail_acct" keyword is not set to "root" and/or other accounts for security personnel, the "action_mail_acct" keyword is missing, or the retuned line is commented out, ask the SA to indicate how they and the ISSO are notified of an audit process failure.

If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

Internal Only - General

Remediation:

Configure the "auditd" service to notify the SA and ISSO in the event of an audit processing failure.

Edit the following line in "/etc/audit/auditd.conf" to ensure that administrators are notified via email for those situations:

```
action_mail_acct = root
```

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

Internal Only - General

1.208 OL08-00-030030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 Information System Security Officer (ISSO) and System Administrator (SA) (at a minimum) must have mail aliases to be notified of an audit processing failure.

```
GROUP ID: V-248725
RULE ID: SV-248725r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify the administrators are notified in the event of an audit processing failure.

Check that the "/etc/aliases" file has a defined value for "root".

```
$ sudo grep "postmaster:\s*root$" /etc/aliases

postmaster:  root
```

If the command does not return a line or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to notify administrators in the event of an audit processing failure.

Add/update the following line in "/etc/aliases":

```
postmaster: root
```


Internal Only - General

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

Internal Only - General

1.209 OL08-00-030040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 System must take appropriate action when an audit processing failure occurs.

```
GROUP ID: V-248726
RULE ID: SV-248726r1038966
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify OL 8 takes the appropriate action when an audit processing failure occurs with the following command:

```
$ sudo grep disk_error_action /etc/audit/auditd.conf

disk_error_action = HALT
```

If the value of the "disk_error_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line ("disk_error_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in the "/etc/audit/auditd.conf" file:

```
disk_error_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the ISSO, configure OL 8 to notify system administration staff and ISSO staff in the event of an audit processing failure by setting the "disk_error_action" to "SYSLOG".

Internal Only - General

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

Internal Only - General

1.210 OL08-00-030060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit system must take appropriate action when the audit storage volume is full.

```
GROUP ID: V-248728
RULE ID: SV-248728r1038966
```

Rationale:

It is critical that when OL 8 is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend on the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, OL 8 must continue generating audit records if possible (automatically restarting the audit service if necessary) and overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, OL 8 must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Audit:

Verify OL 8 takes the appropriate action when the audit storage volume is full with the following command:

```
$ sudo grep disk_full_action /etc/audit/auditd.conf

disk_full_action = HALT
```

If the value of the "disk_full_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line ("disk_full_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in the "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the ISSO, configure OL 8 to notify system administration staff and ISSO staff in the event of an audit processing failure by setting the "disk_full_action" to "SYSLOG".

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

Internal Only - General

1.211 OL08-00-030061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit system must audit local events.

```
GROUP ID: V-248729
RULE ID: SV-248729r991589
```

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Audit:

Verify the OL 8 Audit Daemon is configured to include local events, with the following command:

```
$ sudo grep local_events /etc/audit/auditd.conf

local_events = yes
```

If the value of the "local_events" option is not set to "yes", or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to audit local events on the system.

Add or update the following line in "/etc/audit/auditd.conf" file:

```
local_events = yes
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.212 OL08-00-030062 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must label all offloaded audit logs before sending them to the central log server.

```
GROUP ID: V-248730
RULE ID: SV-248730r958754
```

Rationale:

Without establishing what type of events occurred and their source, location, and outcome, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging is needed to determine who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Audit:

Verify the OL 8 audit daemon is configured to label all offloaded audit logs with the following command:

```
$ sudo grep "name_format" /etc/audit/auditd.conf

name_format = hostname
```

If the "name_format" option is not "hostname", "fqd", or "numeric", or the line is commented out, this is a finding.

Remediation:

Edit the "/etc/audit/auditd.conf" file and add or update the "name_format" option:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect.

Internal Only - General

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

Internal Only - General

1.213 OL08-00-030063 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must resolve audit information before writing to disk.

```
GROUP ID: V-248731
RULE ID: SV-248731r991589
```

Rationale:

Without establishing what type of events occurred and their source, location, and outcome, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging aids in making sense of who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

Audit:

Verify the OL 8 audit daemon is configured to resolve audit information before writing to disk, with the following command:

```
$ sudo grep "log_format" /etc/audit/auditd.conf

log_format = ENRICHED
```

If the "log_format" option is not "ENRICHED", or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to resolve audit information before writing to disk by adding the following line to the "/etc/audit/auditd.conf" file and add or update the "log_format" option:

```
log_format = ENRICHED
```

The audit daemon must be restarted for changes to take effect.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.214 OL08-00-030070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit logs must have a mode of "0600" or less permissive to prevent unauthorized read access.

```
GROUP ID: V-248732
RULE ID: SV-248732r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit logs have a mode of "0600" or less permissive.

Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log has a mode of "0600" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /var/log/audit/audit.log

600 /var/log/audit/audit.log
```

If the audit log has a mode more permissive than "0600", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct permissive mode with the following command:

```
$ sudo chmod 0600 [audit_log_file]
```

Replace "[audit_log_file]" to the correct audit log path. By default, this location is "/var/log/audit/audit.log".

Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.215 OL08-00-030080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit logs must be owned by root to prevent unauthorized read access.

```
GROUP ID: V-248733
RULE ID: SV-248733r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit logs are owned by "root".

Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log is owned by "root" using the following command:

```
$ sudo ls -al /var/log/audit/audit.log

rw------- 2 root root 23 Jun 11 11:56 /var/log/audit/audit.log
```

If the audit log is not owned by "root", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct owner as "root" with the following command:

```
$ sudo chown root [audit_log_file]
```

Replace "[audit_log_file]" to the correct audit log path. By default, this location is "/var/log/audit/audit.log".

Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.216 OL08-00-030090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit logs must be group-owned by root to prevent unauthorized read access.

```
GROUP ID: V-248734
RULE ID: SV-248734r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit logs are group-owned by "root".

Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log is group-owned by "root" using the following command:

```
$ sudo ls -al /var/log/audit/audit.log

rw------- 2 root root 23 Jun 11 11:56 /var/log/audit/audit.log
```

If the audit log is not group-owned by "root", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct group-owner as "root" with the following command:

```
$ sudo chgrp root [audit_log_file]
```

Replace "[audit_log_file]" to the correct audit log path. By default, this location is "/var/log/audit/audit.log".

Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.217 OL08-00-030100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit log directory must be owned by root to prevent unauthorized read access.

```
GROUP ID: V-248735
RULE ID: SV-248735r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log directory is owned by "root" to prevent unauthorized read access.

Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Determine the owner of the audit log directory by using the output of the above command (ex: "/var/log/audit/"). Run the following command with the correct audit log directory path:

```
$ sudo ls -ld /var/log/audit

drwx------ 2 root root 23 Jun 11 11:56 /var/log/audit
```

If the audit log directory is not owned by "root", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct owner as "root" with the following command:

```
$ sudo chown root [audit_log_directory]
```

Replace "[audit_log_directory]" with the correct audit log directory path. By default, this location is usually "/var/log/audit".

Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.218 OL08-00-030110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit log directory must be group-owned by root to prevent unauthorized read access.

```
GROUP ID: V-248736
RULE ID: SV-248736r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log directory is group-owned by "root" to prevent unauthorized read access.

Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Determine the group owner of the audit log directory by using the output of the above command (ex: "/var/log/audit/"). Run the following command with the correct audit log directory path:

```
$ sudo ls -ld /var/log/audit

drwx------ 2 root root 23 Jun 11 11:56 /var/log/audit
```

If the audit log directory is not group-owned by "root", this is a finding.

Internal Only - General

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct group-owner as "root" with the following command:

```
$ sudo chgrp root [audit_log_directory]
```

Replace "[audit_log_directory]" with the correct audit log directory path. By default, this location is usually "/var/log/audit".

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.219 OL08-00-030120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit log directory must have a mode of 0700 or less permissive to prevent unauthorized read access.

```
GROUP ID: V-248737
RULE ID: SV-248737r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the location of the audit log, determine the directory where the audit logs are stored (ex: "/var/log/audit"). Run the following command to determine the permissions for the audit log folder:

```
$ sudo stat -c "%a %n" /var/log/audit

700 /var/log/audit
```

If the audit log directory has a mode more permissive than "0700", this is a finding.

Remediation:

Configure the audit log directory to be protected from unauthorized read access by setting the correct permissive mode with the following command:

```
$ sudo chmod 0700 [audit_log_directory]
```

Replace "[audit_log_directory]" to the correct audit log directory path. By default, this location is "/var/log/audit".

Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.220 OL08-00-030121 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit system must protect auditing rules from unauthorized change.

```
GROUP ID: V-248738
RULE ID: SV-248738r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 system activity.

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. A system reboot would be noticeable and a system administrator could then investigate the unauthorized changes.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit system prevents unauthorized changes with the following command:

```
$ sudo grep "^\s*[^#]" /etc/audit/audit.rules | tail -1

-e 2
```

If the audit system is not set to be immutable by adding the "-e 2" option to the "/etc/audit/audit.rules", this is a finding.

Remediation:

Configure the audit system to set the audit rules to be immutable by adding the following line to "/etc/audit/rules.d/audit.rules":

```
-e 2
```

Note: Once set, the system must be rebooted for auditing to be changed. It is recommended to add this option as the last step in securing the system.

Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.221 OL08-00-030122 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit system must protect logon UIDs from unauthorized change.

```
GROUP ID: V-248739
RULE ID: SV-248739r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit OL 8 system activity.

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. A system reboot would be noticeable and a system administrator could then investigate the unauthorized changes.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit system prevents unauthorized changes to logon UIDs with the following command:

```
$ sudo grep -i immutable /etc/audit/audit.rules

--loginuid-immutable
```

If the login UIDs are not set to be immutable by adding the "--loginuid-immutable" option to the "/etc/audit/audit.rules", this is a finding.

Remediation:

Configure the audit system to set the logon UIDs to be immutable by adding the following line to "/etc/audit/rules.d/audit.rules":

```
--loginuid-immutable
```


Internal Only - General

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.222 OL08-00-030130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creation events that affect "/etc/shadow".

```
GROUP ID: V-248740
RULE ID: SV-248740r1015064
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/shadow /etc/audit/audit.rules

-w /etc/shadow -p wa -k identity
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations events that affect "/etc/shadow".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/shadow -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

Internal Only - General

CCI-001404 Automatically audit account disabling actions.
- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.
- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.
- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.
- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.223 OL08-00-030140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creation events that affect "/etc/security/opasswd".

```
GROUP ID: V-248741
RULE ID: SV-248741r1015065
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/security/opasswd /etc/audit/audit.rules

-w /etc/security/opasswd -p wa -k identity
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations events that affect "/etc/security/opasswd".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/security/opasswd -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```


Internal Only - General

Additional Information:
CCI-000018 Automatically audit account creation actions.
- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.
- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.
- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.
- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.
- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.
- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

Internal Only - General

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.224 OL08-00-030150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creation events that affect "/etc/passwd".

```
GROUP ID: V-248742
RULE ID: SV-248742r1015066
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/passwd /etc/audit/audit.rules

-w /etc/passwd -p wa -k identity
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations events that affect "/etc/passwd".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/passwd -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.225 OL08-00-030160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creation events that affect "/etc/gshadow".

```
GROUP ID: V-248743
RULE ID: SV-248743r1015067
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/gshadow /etc/audit/audit.rules

-w /etc/gshadow -p wa -k identity
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations events that affect "/etc/gshadow".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/gshadow -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000018 Automatically audit account creation actions.
- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.
- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.
- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.
- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.
- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

Internal Only - General

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.226 OL08-00-030170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creation events that affect "/etc/group".

```
GROUP ID: V-248744
RULE ID: SV-248744r1015068
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations events that affect "/etc/group".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/group /etc/audit/audit.rules

-w /etc/group -p wa -k identity
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations events that affect "/etc/group".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/group -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.227 OL08-00-030171 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".

```
GROUP ID: V-248745
RULE ID: SV-248745r1015069
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/sudoers /etc/audit/audit.rules

-w /etc/sudoers -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

```
$ sudo service auditd restart
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.228 OL08-00-030172 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".

```
GROUP ID: V-248746
RULE ID: SV-248746r1015070
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000476-GPOS-00221

Audit:

Verify OL 8 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep /etc/sudoers.d/ /etc/audit/audit.rules

-w /etc/sudoers.d/ -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers.d/ -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

```
$ sudo service auditd restart
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

Internal Only - General

1.229 OL08-00-030180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit package must be installed.

```
GROUP ID: V-248519
RULE ID: SV-248519r1015024
```

Rationale:

Without establishing what type of events occurred and their source, location, and outcome, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in OL 8 audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured OL 8 system.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000062-GPOS-00031, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220

Audit:

Verify the audit service is configured to produce audit records.

Check that the audit service is installed with the following command:

```
$ sudo yum list installed audit
```

If the "auditd" package is not installed, this is a finding.

Internal Only - General

Remediation:

Configure the audit service to produce audit records containing the information needed to establish when (date and time) an event occurred.

Install the audit service (if the audit service is not already installed) with the following command:

```
$ sudo yum install audit
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

CCI-000133 Ensure that audit records containing information that establishes the source of the event.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.
- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.
- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 f

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

Internal Only - General

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.
- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.
- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.
- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.
- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.
- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.
- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.
- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.
- NIST SP 800-53 Revision 4::AU-12 (3)
- NIST SP 800-53 Revision 5::AU-12 (3)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.
- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-001814 The Information system supports auditing of the enforcement actions.
- NIST SP 800-53 Revision 4::CM-5 (1)

Internal Only - General

1.230 OL08-00-030181 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit records must contain information to establish what type of events occurred, the source of events, where events occurred, and the outcome of events.

```
GROUP ID: V-248520
RULE ID: SV-248520r1015025
```

Rationale:

Without establishing what type of events occurred and their source, location, and outcome, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in OL 8 audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured OL 8 system.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000062-GPOS-00031, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220

Internal Only - General

Audit:

Verify the audit service is configured to produce audit records with the following command:

```
$ sudo systemctl status auditd.service

auditd.service - Security Auditing Service
Loaded:loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor
preset: enabled)
Active: active (running) since Tues 2020-12-11 12:56:56 EST; 4 weeks 0 days
ago
```

If the audit service is not "active" and "running", this is a finding.

Remediation:

Configure the audit service to produce audit records containing the information needed to establish when (date and time) an event occurred with the following commands:

```
$ sudo systemctl enable auditd.service
$ sudo systemctl start auditd.service
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

Internal Only - General

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)

Internal Only - General

- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 f

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4::AU-7 a

Internal Only - General

- NIST SP 800-53 Revision 5::AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4::AU-12 (3)
- NIST SP 800-53 Revision 5::AU-12 (3)

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5::MA-3 (5)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

Internal Only - General

1.231 OL08-00-030190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "su" command.

```
GROUP ID: V-248747
RULE ID: SV-248747r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "su" command allows a user to run commands with a substitute user and group ID.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates audit records for any use of the "su" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -iw /usr/bin/su /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k
privileged-priv_change
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to generate audit records for any use of the "su" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.232 OL08-00-030200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit system must be configured to audit any use of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls.

```
GROUP ID: V-248748
RULE ID: SV-248748r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). "Setxattr" is a system call used to set an extended attribute value. "Fsetxattr" is a system call used to set an extended attribute value. This is used to set extended attributes on a file. "Lsetxattr" is a system call used to set an extended attribute value. This is used to set extended attributes on a symbolic link. "Removexattr" is a system call that removes extended attributes. "Fremovexattr" is a system call that removes extended attributes. This is used for removal of extended attributes from a file. "Lremovexattr" is a system call that removes extended attributes. This is used for removal of extended attributes from symbolic links.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. Performance can be helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000466-GPOS-00210, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219

Internal Only - General

Audit:

Verify if OL 8 is configured to audit the execution of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls by running the following command:

```
$ sudo grep xattr /etc/audit/audit.rules

-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod

-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
```

If the command does not return an audit rule for "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" or any of the lines returned are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure OL 8 to audit the execution of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod

-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```


Internal Only - General

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.233 OL08-00-030250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "chage" command.

```
GROUP ID: V-248753
RULE ID: SV-248753r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chage" command is used to change or view user password expiry information.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "chage" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w chage /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-chage
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "chage" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-chage
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.234 OL08-00-030260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any uses of the "chcon" command.

```
GROUP ID: V-248754
RULE ID: SV-248754r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chcon" command is used to change file SELinux security context.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "chcon" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w chcon /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "chcon" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.235 OL08-00-030280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "ssh-agent" command.

```
GROUP ID: V-248756
RULE ID: SV-248756r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "ssh-agent" is a program to hold private keys used for public key authentication.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "ssh-agent" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep ssh-agent /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-ssh
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "ssh-agent" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.236 OL08-00-030290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "passwd" command.

```
GROUP ID: V-248757
RULE ID: SV-248757r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "passwd" command is used to change passwords for user accounts.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "passwd" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w passwd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "passwd" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.237 OL08-00-030300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "mount" command.

```
GROUP ID: V-248758
RULE ID: SV-248758r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "mount" command is used to mount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "mount" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w /usr/bin/mount /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "mount" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.238 OL08-00-030301 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "umount" command.

```
GROUP ID: V-248759
RULE ID: SV-248759r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "mount" command is used to mount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "umount" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w /usr/bin/umount /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "umount" command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.239 OL08-00-030302 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "mount" syscall.

```
GROUP ID: V-248760
RULE ID: SV-248760r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "mount" command is used to mount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "mount" syscall by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w mount /etc/audit/audit.rules

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "mount" syscall by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.240 OL08-00-030310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "unix_update" command.

```
GROUP ID: V-248761
RULE ID: SV-248761r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. "Unix_update" is a helper program for the "pam_unix" module that updates the password for a given user. It is not intended to be run directly from the command line and logs a security violation in that event.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "unix_update" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "unix_update" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "unix_update" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.241 OL08-00-030311 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "postdrop" command.

```
GROUP ID: V-248762
RULE ID: SV-248762r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "postdrop" command creates a file in the maildrop directory and copies its standard input to the file.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "postdrop" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "postdrop" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any use of the "postdrop" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

Internal Only - General

```
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.242 OL08-00-030312 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "postqueue" command.

```
GROUP ID: V-248763
RULE ID: SV-248763r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "postqueue" command implements the Postfix user interface for queue management.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "postqueue" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "postqueue" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "postqueue" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.243 OL08-00-030313 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "semanage" command.

```
GROUP ID: V-248764
RULE ID: SV-248764r958442
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "semanage" command is used to configure certain elements of SELinux policy without requiring modification to or recompilation from policy sources.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Audit:

Verify if OL 8 is configured to audit the execution of the "semanage" command by running the following command:

```
$ sudo grep -w semanage /etc/audit/audit.rules

a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return all lines or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to audit the execution of the "semanage" command by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

1.244 OL08-00-030314 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "setfiles" command.

```
GROUP ID: V-248765
RULE ID: SV-248765r958442
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "setfiles" command is primarily used to initialize the security context fields (extended attributes) on one or more filesystems (or parts of them). Usually it is initially run as part of the SELinux installation process (a step commonly known as labeling).

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Audit:

Verify OL 8 is configured to audit the execution of the "setfiles" command by running the following command:

```
$ sudo grep -w setfiles /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return all lines or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to audit the execution of the "setfiles" command by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

1.245 OL08-00-030315 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "userhelper" command.

```
GROUP ID: V-248766
RULE ID: SV-248766r958442
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "userhelper" command is not intended to be run interactively. "Userhelper" provides a basic interface to change a user's password, gecos information, and shell. The main difference between this program and its traditional equivalents (passwd, chfn, chsh) is that prompts are written to standard out to make it easy for a graphical user interface wrapper to interface to it as a child process.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Audit:

Verify OL 8 is configured to audit the execution of the "userhelper" command by running the following command:

```
$ sudo grep -w userhelper /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return all lines or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to audit the execution of the "userhelper" command by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

1.246 OL08-00-030316 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "setsebool" command.

```
GROUP ID: V-248767
RULE ID: SV-248767r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "setsebool" command sets the current state of a particular SELinux boolean or a list of booleans to a given value.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 is configured to audit the execution of the "setsebool" command by running the following command:

```
$ sudo grep -w setsebool /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return all lines or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to audit the execution of the "setsebool" command by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.247 OL08-00-030317 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "unix_chkpwd" command.

```
GROUP ID: V-248768
RULE ID: SV-248768r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "unix_chkpwd" command is a helper program for the pam_unix module that verifies the password of the current user. It also checks password and account expiration dates in shadow. It is not intended to be run directly from the command line and logs a security violation if done so.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 is configured to audit the execution of the "unix_chkpwd" command by running the following command:

```
$ sudo grep -w unix_chkpwd /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return all lines or the lines are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure OL 8 to audit the execution of the "unix_chkpwd" command by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.248 OL08-00-030320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "ssh-keysign" command.

```
GROUP ID: V-248769
RULE ID: SV-248769r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "ssh-keysign" program is an SSH helper program for host-based authentication.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of "ssh-keysign" by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep ssh-keysign /etc/audit/audit.rules

-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=unset -k privileged-ssh
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of "ssh-keysign" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=unset -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.249 OL08-00-030330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "setfacl" command.

```
GROUP ID: V-248770
RULE ID: SV-248770r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "setfacl" command is used to set file access control lists.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "setfacl" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w setfacl /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "setfacl" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.250 OL08-00-030340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "pam_timestamp_check" command.

```
GROUP ID: V-248771
RULE ID: SV-248771r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "pam_timestamp_check" command is used to check if the default timestamp is valid.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "pam_timestamp_check" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w pam_timestamp_check /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000
-F auid!=unset -k privileged-pam_timestamp_check
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "pam_timestamp_check" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000
-F auid!=unset -k privileged-pam_timestamp_check
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.251 OL08-00-030350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "newgrp" command.

```
GROUP ID: V-248772
RULE ID: SV-248772r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "newgrp" command is used to change the current group ID during a login session.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "newgrp" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w newgrp /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset
-k priv_cmd
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "newgrp" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset
-k priv_cmd
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.252 OL08-00-030360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "init_module" and "finit_module" system calls.

```
GROUP ID: V-248773
RULE ID: SV-248773r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "init_module" and "finit_module" system calls are used to load a kernel module.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. Performance can be helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Internal Only - General

Audit:

Verify OL 8 generates an audit record for any use of the "init_module" and "finit_module" system calls by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep init_module /etc/audit/audit.rules

-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k module_chng
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k module_chng
```

If the command does not return an audit rule for "init_module" and "finit_module" or any of the lines returned are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any use of the "init_module" and "finit_module" system calls by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k module_chng
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k module_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.253 OL08-00-030361 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls.

```
GROUP ID: V-248774
RULE ID: SV-248774r1069140
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "rename" system call will rename the specified files by replacing the first occurrence of expression in their name by replacement. The "unlink" system call deletes a name from the filesystem. If that name was the last link to a file and no processes have the file open, the file is deleted and the space it was using is made available for reuse. The "rmdir" system call removes empty directories. The "renameat" system call renames a file, moving it between directories, if required. The "unlinkat" system call operates in exactly the same way as either "unlink" or "rmdir" except for the differences described in the manual page.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. Performance can be helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Internal Only - General

Audit:

Verify OL 8 is configured to generate audit records for any use of the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls by running the following command:

```
$ sudo grep 'rename\|unlink\|rmdir' /etc/audit/audit.rules

-a always,exit -F arch=b32 -S rename,unlink,rmdir,renameat,unlinkat -F
auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S rename,unlink,rmdir,renameat,unlinkat -F
auid>=1000 -F auid!=unset -k delete
```

If the command does not return an audit rule for "rename", "unlink", "rmdir", "renameat" and "unlinkat" or any of the lines returned are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure OL 8 to generate audit records for any use of the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S rename,unlink,rmdir,renameat,unlinkat -F
auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S rename,unlink,rmdir,renameat,unlinkat -F
auid>=1000 -F auid!=unset -k delete
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.254 OL08-00-030370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "gpasswd" command.

```
GROUP ID: V-248779
RULE ID: SV-248779r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "gpasswd" command is used to administer "/etc/group" and "/etc/gshadow". Every group can have administrators, members, and a password.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "gpasswd" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w gpasswd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-gpasswd
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "gpasswd" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-gpasswd
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.255 OL08-00-030390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the delete_module syscall.

```
GROUP ID: V-248781
RULE ID: SV-248781r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "delete_module" command is used to unload a kernel module.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "delete_module" syscall by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "delete_module" /etc/audit/audit.rules

-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "delete_module" syscall by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.256 OL08-00-030400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "crontab" command.

```
GROUP ID: V-248782
RULE ID: SV-248782r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "crontab" command is used to maintain crontab files for individual users. Crontab is the program used to install, remove, or list the tables used to drive the cron daemon. This is similar to the task scheduler used in other operating systems.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "crontab" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w crontab /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-crontab
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "crontab" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-crontab
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.257 OL08-00-030410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "chsh" command.

```
GROUP ID: V-248783
RULE ID: SV-248783r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chsh" command is used to change the login shell.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "chsh" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w chsh /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "chsh" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.258 OL08-00-030420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls.

```
GROUP ID: V-248784
RULE ID: SV-248784r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "truncate" and "ftruncate" functions are used to truncate a file to a specified length. The "creat" system call is used to open and possibly create a file or device. The "open" system call opens a file specified by a pathname. If the specified file does not exist, it may optionally be created by "open". The "openat" system call opens a file specified by a relative pathname. The "name_to_handle_at" and "open_by_handle_at" system calls split the functionality of openat into two parts: "name_to_handle_at" returns an opaque handle that corresponds to a specified file; "open_by_handle_at" opens the file corresponding to a handle returned by a previous call to "name_to_handle_at" and returns an open file descriptor.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. Performance can be helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Internal Only - General

Audit:

Verify OL 8 generates an audit record for any use of the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep 'open\|truncate\|creat' /etc/audit/audit.rules

-a always,exit -F arch=b32 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access

-a always,exit -F arch=b32 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
```

If the output does not produce rules containing "-F exit=-EPERM", this is a finding.

If the output does not produce rules containing "-F exit=-EACCES", this is a finding.

If the command does not return an audit rule for "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" or any of the lines returned are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access

-a always,exit -F arch=b32 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

Internal Only - General

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.259 OL08-00-030480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "chown", "fchown", "fchownat", and "lchown" system calls.

```
GROUP ID: V-248790
RULE ID: SV-248790r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chown" command is used to change file owner and group. The "fchown" system call is used to change the ownership of a file referred to by the open file descriptor. The "fchownat" system call is used to change ownership of a file relative to a directory file descriptor. The "lchown" system call is used to change the ownership of the file specified by a path, which does not dereference symbolic links.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. Performance can be helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Internal Only - General

Audit:

Verify OL 8 generates an audit record for any use of the "chown", "fchown", "fchownat", and "lchown" system calls by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep chown /etc/audit/audit.rules

-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=unset -k perm_chng
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=unset -k perm_chng

If audit rules are not defined for "chown", "fchown", "fchownat", and
"lchown" or any of the lines returned are commented out, this is a finding.
```

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any use of the "chown", "fchown", "fchownat", and "lchown" system calls by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=unset -k perm_chng
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=unset -k perm_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.260 OL08-00-030490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "chmod", "fchmod", and "fchmodat" system calls.

```
GROUP ID: V-248791
RULE ID: SV-248791r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chmod" system call changes the file mode bits of each given file according to mode, which can be either a symbolic representation of changes to make or an octal number representing the bit pattern for the new mode bits. The "fchmod" system call is used to change permissions of a file. The "fchmodat" system call is used to change permissions of a file relative to a directory file descriptor.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each syscall that all programs on the system makes. Therefore, it is very important to only use syscall rules when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. Performance can be helped, though, by combining syscalls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Internal Only - General

Audit:

Verify OL 8 generates an audit record for any use of the "chmod","fchmod", and "fchmodat" syscalls by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep chmod /etc/audit/audit.rules

-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -k perm_chng
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -k perm_chng
```

If the command does not return an audit rule for "chmod", "fchmod", and "fchmodat", or any of the lines returned are commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any use of the "chmod", "fchmod", and "fchmodat" syscalls by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -k perm_chng
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -k perm_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.261 OL08-00-030550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "sudo" command.

```
GROUP ID: V-248797
RULE ID: SV-248797r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "sudo" command allows a permitted user to execute a command as the superuser or another user as specified by the security policy.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "sudo" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w sudo /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "sudo" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.262 OL08-00-030560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "usermod" command.

```
GROUP ID: V-248798
RULE ID: SV-248798r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "usermod" command modifies the system account files to reflect the changes that are specified on the command line.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit event for any use of the "usermod" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w usermod /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-usermod
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "usermod" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-usermod
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.263 OL08-00-030570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "chacl" command.

```
GROUP ID: V-248799
RULE ID: SV-248799r958412
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chacl" command is used to change the access control list of a file or directory.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Audit:

Verify OL 8 generates an audit record for any use of the "chacl" command by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w chacl /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Internal Only - General

Remediation:

Configure the audit system to generate an audit event for any use of the "chacl" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.264 OL08-00-030580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any use of the "kmod" command.

```
GROUP ID: V-248800
RULE ID: SV-248800r958412
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "kmod" command is used to control Linux Kernel modules.

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which OL 8 will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Internal Only - General

Audit:

Verify OL 8 is configured to audit the execution of the module management program "kmod" by running the following command:

```
$ sudo grep "/usr/bin/kmod" /etc/audit/audit.rules

-w /usr/bin/kmod -p x -k modules
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure OL 8 to audit the execution of the module management program "kmod" by adding or updating the following line to "/etc/audit/rules.d/audit.rules":

```
-w /usr/bin/kmod -p x -k modules
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.265 OL08-00-030590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any attempted modifications to the "faillock" log file.

```
GROUP ID: V-248801
RULE ID: SV-248801r958412
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which OL 8 will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

From "Pam_Faillock man" pages: Note the default directory that "pam_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Internal Only - General

Audit:

Verify OL 8 generates an audit record for any attempted modifications to the "faillock" file.

Determine where the faillock tallies are stored with the following commands:

For OL versions 8.0 and 8.1:

```
$ sudo grep -i pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent deny=3
fail_interval=900 even_deny_root
```

For OL versions 8.2 and newer:

```
$ sudo grep dir /etc/security/faillock.conf

dir=/var/log/faillock
```

Using the location of the faillock log file, check that the following calls are being audited by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w faillock /etc/audit/audit.rules

-w /var/log/faillock -p wa -k logins
```

If the command does not return a line or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any attempted modifications to the "faillock" file by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-w /var/log/faillock -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```


Internal Only - General

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.266 OL08-00-030600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must generate audit records for any attempted modifications to the "lastlog" file.

```
GROUP ID: V-248802
RULE ID: SV-248802r958412
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which OL 8 will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Internal Only - General

Audit:

Verify OL 8 generates an audit record for any attempted modifications to the "lastlog" file by running the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w lastlog /etc/audit/audit.rules

-w /var/log/lastlog -p wa -k logins
```

If the command does not return a line or the line is commented out, this is a finding.

Note: The "-k" allows for specifying an arbitrary identifier, and the string after it does not need to match the example output above.

Remediation:

Configure the audit system to generate an audit event for any attempted modifications to the "lastlog" file by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-w /var/log/lastlog -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect. To restart the audit daemon, run the following command:

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.267 OL08-00-030601 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable auditing of processes that start prior to the audit daemon.

```
GROUP ID: V-248803
RULE ID: SV-248803r958412
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which OL 8 will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Internal Only - General

Audit:

Verify OL 8 enables auditing of processes that start prior to the audit daemon with the following commands:

```
$ sudo grub2-editenv list | grep audit

kernelopts=root=/dev/mapper/ol-root ro crashkernel=auto
resume=/dev/mapper/ol-swap rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb quiet
fips=1 audit=1 audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-ba41-
1c021ac29e82
```

If the "audit" entry does not equal "1", is missing, or the line is commented out, this is a finding.

Check that auditing is enabled by default to persist in kernel updates:

```
$ sudo grep audit /etc/default/grub

GRUB_CMDLINE_LINUX="audit=1"
```

If "audit" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure OL 8 to audit processes that start prior to the audit daemon with the following command:

```
$ sudo grubby --update-kernel=ALL --args="audit=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="audit=1"
```

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

Internal Only - General

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.268 OL08-00-030602 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must allocate an "audit_backlog_limit" of sufficient size to capture processes that start prior to the audit daemon.

```
GROUP ID: V-248804
RULE ID: SV-248804r958412
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Allocating an "audit_backlog_limit" of sufficient size is critical in maintaining a stable boot process. With an insufficient limit allocated, the system is susceptible to boot failures and crashes.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Internal Only - General

Audit:

Verify OL 8 allocates a sufficient "audit_backlog_limit" to capture processes that start prior to the audit daemon with the following commands:

```
$ sudo grub2-editenv list | grep audit

kernelopts=root=/dev/mapper/ol-root ro crashkernel=auto
resume=/dev/mapper/ol-swap rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb quiet
fips=1 audit=1 audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-ba41-
1c021ac29e82
```

If the "audit_backlog_limit" entry does not equal "8192" or larger, is missing, or the line is commented out, this is a finding.

Verify "audit_backlog_limit" is set to persist in kernel updates:

```
$ sudo grep audit /etc/default/grub

GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

If "audit_backlog_limit" is not set to "8192" or larger or is missing or commented out, this is a finding.

Remediation:

Configure OL 8 to allocate sufficient "audit_backlog_limit" to capture processes that start prior to the audit daemon with the following command:

```
$ sudo grubby --update-kernel=ALL --args="audit_backlog_limit=8192"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient space will need be to be created.

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

Internal Only - General

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

Internal Only - General

1.269 OL08-00-030603 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable Linux audit logging for the USBGuard daemon.

```
GROUP ID: V-248805
RULE ID: SV-248805r991579
```

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify OL 8 enables Linux audit logging of the USBGuard daemon with the following commands.

Note: If the USBGuard daemon is not installed and enabled, this requirement is not applicable.

```
$ sudo grep -i auditbackend /etc/usbguard/usbguard-daemon.conf

AuditBackend=LinuxAudit
```

If the "AuditBackend" entry does not equal "LinuxAudit", is missing, or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to enable Linux audit logging of the USBGuard daemon by adding or modifying the following line in "/etc/usbguard/usbguard-daemon.conf":

```
AuditBackend=LinuxAudit
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

Internal Only - General

1.270 OL08-00-030610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must allow only the Information System Security Manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.

```
GROUP ID: V-248806
RULE ID: SV-248806r958444
```

Rationale:

Without the capability to restrict the roles and individuals that can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify the "/etc/audit/rules.d/*.rules" and "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive by using the following commands:

```
$ sudo ls -al /etc/audit/rules.d/*.rules

-rw-r----- 1 root root 1280 Feb 16 17:09 audit.rules
$ sudo ls -al /etc/audit/auditd.conf

-rw-r----- 1 root root 621 Sep 22 2014 auditd.conf
```

If the "/etc/audit/rules.d/*.rules" or "/etc/audit/auditd.conf" files have a mode more permissive than "0640", this is a finding.

Remediation:

Configure the "/etc/audit/rules.d/*.rules" and "/etc/audit/auditd.conf" files to have a mode of "0640" with the following commands:

```
$ sudo chmod 0640 /etc/audit/rules.d/*.rules
$ sudo chmod 0640 /etc/audit/auditd.conf
```

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

Internal Only - General

1.271 OL08-00-030620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit tools must have a mode of "0755" or less permissive.

```
GROUP ID: V-248807
RULE ID: SV-248807r991557
```

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

OL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding user rights, to make access decisions regarding the access to audit tools.

Audit tools include but are not limited to vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode.

Check the octal permission of each audit tool by running the following command:

```
$ sudo stat -c "%a %n" /sbin/auditctl /sbin/aureport /sbin/ausearch
/sbin/autrace /sbin/auditd /sbin/rsyslogd /sbin/augenrules

755 /sbin/auditctl
755 /sbin/aureport
755 /sbin/ausearch
750 /sbin/autrace
755 /sbin/auditd
755 /sbin/rsyslogd
755 /sbin/augenrules
```

If any of the audit tools has a mode more permissive than "0755", this is a finding.

Internal Only - General

Remediation:

Configure the audit tools to be protected from unauthorized access by setting the correct permissive mode using the following command:

```
$ sudo chmod 0755 [audit_tool]
```

Replace "[audit_tool]" with the audit tool that does not have the correct permissive mode.

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.272 OL08-00-030630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit tools must be owned by root.

```
GROUP ID: V-248808
RULE ID: SV-248808r991557
```

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

OL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding user rights, to make access decisions regarding the access to audit tools.

Audit tools include but are not limited to vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

Verify the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification.

Check the owner of each audit tool by running the following command:

```
$ sudo stat -c "%U %n" /sbin/auditctl /sbin/aureport /sbin/ausearch
/sbin/autrace /sbin/auditd /sbin/rsyslogd /sbin/augenrules

root /sbin/auditctl
root /sbin/aureport
root /sbin/ausearch
root /sbin/autrace
root /sbin/auditd
root /sbin/rsyslogd
root /sbin/augenrules
```

If any of the audit tools are not owned by "root", this is a finding.

Internal Only - General

Remediation:

Configure the audit tools to be owned by "root" by running the following command:

```
$ sudo chown root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not owned by "root".

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.273 OL08-00-030640 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 audit tools must be group-owned by root.

```
GROUP ID: V-248809
RULE ID: SV-248809r991557
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

OL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding user rights, to make access decisions regarding the access to audit tools.

Audit tools include but are not limited to vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

Verify the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification.

Check the owner of each audit tool by running the following commands:

```
$ sudo stat -c "%G %n" /sbin/auditctl /sbin/aureport /sbin/ausearch
/sbin/autrace /sbin/auditd /sbin/rsyslogd /sbin/augenrules

root /sbin/auditctl
root /sbin/aureport
root /sbin/ausearch
root /sbin/autrace
root /sbin/auditd
root /sbin/rsyslogd
root /sbin/augenrules
```

If any of the audit tools are not group-owned by "root", this is a finding.

Internal Only - General

Remediation:

Configure the audit tools to be group-owned by "root" by running the following command:

```
$ sudo chgrp root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not group-owned by "root".

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

Internal Only - General

1.274 OL08-00-030650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must use cryptographic mechanisms to protect the integrity of audit tools.

```
GROUP ID: V-248810
RULE ID: SV-248810r991567
```

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include but are not limited to vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools to provide the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools.

Check the selection lines to ensure AIDE is configured to add/check with the following command:

```
$ sudo grep -E '(\/usr\/sbin\/(audit|au|rsys))' /etc/aide.conf

/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/rsyslogd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

If any of the audit tools listed above do not have an appropriate selection line, this is a finding.

Internal Only - General

Remediation:

Add or update the following lines to "/etc/aide.conf" to protect the integrity of the audit tools.

```
# Audit Tools
/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/rsyslogd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

Additional Information:

CCI-001496 Implement cryptographic mechanisms to protect the integrity of audit tools.

- NIST SP 800-53::AU-9 (3)
- NIST SP 800-53A::AU-9 (3).1
- NIST SP 800-53 Revision 4::AU-9 (3)
- NIST SP 800-53 Revision 5::AU-9 (3)

Internal Only - General

1.275 OL08-00-030660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must allocate audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

```
GROUP ID: V-248811
RULE ID: SV-248811r958752
```

Rationale:

To ensure OL 8 systems have a sufficient storage capacity in which to write the audit logs, OL 8 needs to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of OL 8.

Internal Only - General

Audit:

Verify OL 8 allocates audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine to which partition the audit records are being written with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Check the size of the partition to which audit records are written (with the example being "/var/log/audit/") with the following command:

```
$ sudo df -h /var/log/audit/

/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit
```

If the audit records are not written to a partition made specifically for audit records ("/var/log/audit" is a separate partition), determine the amount of space being used by other files in the partition with the following command:

```
$ sudo du -sh [audit_partition]

1.8G /var/log/audit
```

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Note: The partition size needed to capture a week of audit records is based on the activity level of the system and the total storage capacity available. Typically 10.0 GB of storage space for audit records should be sufficient.

Remediation:

Allocate enough storage capacity for at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

If audit records are stored on a partition made specifically for audit records, use the "X" program to resize the partition with sufficient space to contain one week of audit records.

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient space will need be to be created.

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

Internal Only - General

1.276 OL08-00-030670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must have the packages required for offloading audit logs installed.

```
GROUP ID: V-248812
RULE ID: SV-248812r991589
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

OL 8 installation media provides "rsyslogd". This is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS, and DTLS protocols) provides a method to securely encrypt and offload auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration follow: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514

Note that a port number was given as there is no standard port for RELP.

Audit:

Verify the operating system has the packages required for offloading audit logs installed with the following commands:

```
$ sudo yum list installed rsyslog

rsyslog.x86_64 8.1911.0-3.el8 @AppStream
```

If the "rsyslog" package is not installed, ask the administrator to indicate how audit logs are being offloaded and what packages are installed to support it.

If there is no evidence of audit logs being offloaded, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to offload audit logs by installing the required packages with the following command:

```
$ sudo yum install rsyslog
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.277 OL08-00-030680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must have the packages required for encrypting offloaded audit logs installed.

```
GROUP ID: V-248813
RULE ID: SV-248813r991589
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

OL 8 installation media provides "rsyslogd". This is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols) provides a method to securely encrypt and offload auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration follow: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514

Note that a port number was given as there is no standard port for RELP.

Audit:

Verify the operating system has the packages required for encrypting offloaded audit logs installed with the following commands:

```
$ sudo yum list installed rsyslog-gnutls

rsyslog-gnutls.x86_64 8.1911.0-6.el8 @AppStream
```

If the "rsyslog-gnutls" package is not installed, ask the administrator to indicate how audit logs are being encrypted during offloading and what packages are installed to support it.

If there is no evidence of audit logs being encrypted during offloading, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to encrypt offloaded audit logs by installing the required packages with the following command:

```
$ sudo yum install rsyslog-gnutls
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.278 OL08-00-030690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 audit records must be offloaded onto a different system or storage media from the system being audited.

```
GROUP ID: V-248814
RULE ID: SV-248814r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

OL 8 installation media provides "rsyslogd". This is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols) provides a method to securely encrypt and offload auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration follow: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514

Note that a port number was given as there is no standard port for RELP.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Internal Only - General

Audit:

Verify the audit system offloads audit records onto a different system or media from the system being audited with the following command:

```
$ sudo grep @@ /etc/rsyslog.conf /etc/rsyslog.d/*.conf

/etc/rsyslog.conf:*.* @@[logaggregationserver.example.mil]:[port]
```

If a remote server is not configured or the line is commented out, ask the system administrator to indicate how the audit logs are offloaded to a different system or media.

If there is no evidence that the audit logs are being offloaded to another system or media, this is a finding.

Remediation:

Configure OL 8 to offload audit records onto a different system or media from the system being audited by specifying the remote logging server in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf" with the name or IP address of the log aggregation server.

For UDP:

```
*.* @[logaggregationserver.example.mil]:[port]
```

For TCP:

```
*.* @@[logaggregationserver.example.mil]:[port]
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

Internal Only - General

1.279 OL08-00-030700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must take appropriate action when the internal event queue is full.

```
GROUP ID: V-248815
RULE ID: SV-248815r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

OL 8 installation media provides "rsyslogd". This is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols) provides a method to securely encrypt and offload auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audit system is configured to take an appropriate action when the internal event queue is full:

```
$ sudo grep -i overflow_action /etc/audit/auditd.conf

overflow_action = syslog
```

If the value of the "overflow_action" option is not set to "syslog", "single", or "halt", or the line is commented out, ask the System Administrator to indicate how the audit logs are offloaded to a different system or media.

If there is no evidence that the transfer of the audit logs being offloaded to another system or media takes appropriate action if the internal event queue becomes full, this is a finding.

Remediation:

Edit the "/etc/audit/auditd.conf" file and add or update the "overflow_action" option:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect.

Internal Only - General

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

Internal Only - General

1.280 OL08-00-030710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must encrypt the transfer of audit records offloaded onto a different system or media from the system being audited.

```
GROUP ID: V-248816
RULE ID: SV-248816r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

OL 8 installation media provides "rsyslogd". This is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS, and DTLS protocols) provides a method to securely encrypt and offload auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Internal Only - General

Audit:

Verify the operating system encrypts audit records offloaded onto a different system or media from the system being audited with the following commands:

```
$ sudo grep -i '$DefaultNetstreamDriver' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$DefaultNetstreamDriver gtls
```

If the value of the "$DefaultNetstreamDriver" option is not set to "gtls" or the line is commented out, this is a finding.

```
$ sudo grep -i '$ActionSendStreamDriverMode' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$ActionSendStreamDriverMode 1
```

If the value of the "$ActionSendStreamDriverMode" option is not set to "1" or the line is commented out, this is a finding.

If neither of the definitions above are set, ask the System Administrator to indicate how the audit logs are offloaded to a different system or media.

If there is no evidence that the transfer of the audit logs being offloaded to another system or media is encrypted, this is a finding.

Remediation:

Configure the operating system to encrypt offloaded audit records by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$DefaultNetstreamDriver gtls
$ActionSendStreamDriverMode 1
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

Internal Only - General

1.281 OL08-00-030720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must authenticate the remote logging server for offloading audit logs.

```
GROUP ID: V-248817
RULE ID: SV-248817r1069157
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

OL 8 installation media provides "rsyslogd". This is a system utility providing support for message logging. Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols) provides a method to securely encrypt and offload auditing.

"Rsyslog" supported authentication modes include the following: anon - anonymous authentication x509/fingerprint - certificate fingerprint authentication x509/certvalid - certificate validation only x509/name - certificate validation and subject name authentication

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Internal Only - General

Audit:

Verify the operating system authenticates the remote logging server for offloading audit logs with the following command:

```
$ sudo grep -i '$ActionSendStreamDriverAuthMode' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$ActionSendStreamDriverAuthMode x509/name
```

If the value of the "$ActionSendStreamDriverAuthMode" option is not set to "x509/name" or the line is commented out, ask the system administrator to indicate how the audit logs are offloaded to a different system or media.

If the variable name "StreamDriverAuthMode" is present in an omfwd statement block, this is not a finding. However, if the "StreamDriverAuthMode" variable is in a module block, this is a finding.

If there is no evidence that the transfer of the audit logs being offloaded to another system or media is encrypted, this is a finding.

Remediation:

Configure the operating system to authenticate the remote logging server for off-loading audit logs by setting the following option in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$ActionSendStreamDriverAuthMode x509/name
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

Internal Only - General

1.282 OL08-00-030730 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-248818
RULE ID: SV-248818r971542
```

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify OL 8 takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following commands:

```
$ sudo grep -w space_left /etc/audit/auditd.conf

space_left = 25%
```

If the value of the "space_left" keyword is not set to "25%" or if the line is commented out, ask the SA to demonstrate how the system is providing real-time alerts to the SA and ISSO.

If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure OL 8 to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the "/etc/audit/auditd.conf" file.

```
space_left = 25%
```


Internal Only - General

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

Internal Only - General

1.283 OL08-00-030731 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated audit record storage volume 75 percent utilization.

```
GROUP ID: V-248819
RULE ID: SV-248819r971542
```

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify OL 8 notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep -w space_left_action /etc/audit/auditd.conf

space_left_action = email
```

If the value of the "space_left_action" is not set to "email", or if the line is commented out, ask the System Administrator to indicate how the system is providing real-time alerts to the SA and ISSO.

If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure the operating system to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

```
space_left_action = email
```

Note: Option names and values in the auditd.conf file are case insensitive.

Internal Only - General

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

Internal Only - General

1.284 OL08-00-030740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must compare internal information system clocks at least every 24 hours with a server synchronized to an authoritative time source, such as the United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

```
GROUP ID: V-248820
RULE ID: SV-248820r1038944
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the operating system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

OL 8 uses the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DOD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit https://www.usno.navy.mil/USNO/time/ntp/dod-customers for more information.

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144, SRG-OS-000359-GPOS-00146

Internal Only - General

Audit:

Verify OL 8 is comparing internal information system clocks at least every 24 hours with an NTP server with the following command:

```
$ sudo grep maxpoll /etc/chrony.conf

server [ntp.server.name] iburst maxpoll 16
```

If the "maxpoll" option is set to a number greater than "16" or the line is commented out, this is a finding.

Remediation:

Configure OL 8 to compare internal information system clocks at least every 24 hours with an NTP server by adding/modifying the following line in the "/etc/chrony.conf" file.

```
server [ntp.server.name] iburst maxpoll 16
```

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

Internal Only - General

1.285 OL08-00-030741 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must disable the chrony daemon from acting as a server.

```
GROUP ID: V-248821
RULE ID: SV-248821r958478
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Minimizing the exposure of the server functionality of the chrony daemon diminishes the attack surface.

Note that USNO offers authenticated NTP service to DOD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit https://www.usno.navy.mil/USNO/time/ntp/DOD-customers for more information.

Audit:

Note: If the system is approved and documented by the information system security officer (ISSO) to function as an NTP time server, this requirement is Not Applicable.

Verify OL 8 disables the chrony daemon from acting as a server with the following command:

```
 $ sudo grep -w 'port' /etc/chrony.conf

 port 0
```

If the "port" option is not set to "0" or is commented out or missing, this is a finding.

Remediation:

Configure OL 8 to disable the chrony daemon from acting as a server by adding or modifying the following line in the "/etc/chrony.conf" file.

```
 port 0
```


Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.286 OL08-00-030742 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must disable network management of the chrony daemon.

```
GROUP ID: V-248822
RULE ID: SV-248822r958478
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Minimizing the exposure of the server functionality of the chrony daemon diminishes the attack surface.

Note that USNO offers authenticated NTP service to DOD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit https://www.usno.navy.mil/USNO/time/ntp/DOD-customers for more information.

Audit:

Note: If the system is approved and documented by the information system security officer (ISSO) to function as an NTP time server, this requirement is Not Applicable.

Verify OL 8 disables network management of the chrony daemon with the following command:

```
$ sudo grep -w 'cmdport' /etc/chrony.conf

cmdport 0
```

If the "cmdport" option is not set to "0" or is commented out or missing, this is a finding.

Remediation:

Configure OL 8 to disable network management of the chrony daemon by adding or modifying the following line in the "/etc/chrony.conf" file.

```
cmdport 0
```


Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.287 OL08-00-040000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must not have the telnet-server package installed.

```
GROUP ID: V-248823
RULE ID: SV-248823r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

The telnet service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Audit:

Determine if the telnet-server package is installed with the following command:

```
$ sudo yum list installed telnet-server
```

If the telnet-server package is installed, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable non-essential capabilities by removing the telnet-server package from the system with the following command:

```
$ sudo yum remove telnet-server
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.288 OL08-00-040001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have any automated bug reporting tools installed.

```
GROUP ID: V-248824
RULE ID: SV-248824r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Audit:

Determine if any automated bug reporting packages are installed with the following command:

```
$ sudo yum list installed abrt*
```

If any automated bug reporting package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing automated bug reporting packages from the system with the following command:

```
$ sudo yum remove abrt*
```


Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.289 OL08-00-040002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the sendmail package installed.

```
GROUP ID: V-248825
RULE ID: SV-248825r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include but are not limited to games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Audit:

Determine if the sendmail package is installed with the following command:

```
$ sudo yum list installed sendmail
```

If the sendmail package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the sendmail package from the system with the following command:

```
$ sudo yum remove sendmail
```


Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.290 OL08-00-040004 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must enable mitigations against processor-based vulnerabilities.

```
GROUP ID: V-248826
RULE ID: SV-248826r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Kernel page-table isolation is a kernel feature that mitigates the Meltdown security vulnerability and hardens the kernel against attempts to bypass kernel address space layout randomization (KASLR).

Internal Only - General

Audit:

Verify OL 8 enables kernel page-table isolation with the following commands:

```
$ sudo grub2-editenv list | grep pti

kernelopts=root=/dev/mapper/ol-root ro crashkernel=auto
resume=/dev/mapper/ol-swap rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb quiet
fips=1 audit=1 audit_backlog_limit=8192 pti=on boot=UUID=8d171156-cd61-421c-
ba41-1c021ac29e82
```

If the "pti" entry does not equal "on", is missing, or the line is commented out, this is a finding.

Check that kernel page-table isolation is enabled by default to persist in kernel updates:

```
$ sudo grep pti /etc/default/grub

GRUB_CMDLINE_LINUX="pti=on"
```

If "pti" is not set to "on", is missing or commented out, this is a finding.

Remediation:

Configure OL 8 to enable kernel page-table isolation with the following command:

```
$ sudo grubby --update-kernel=ALL --args="pti=on"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="pti=on"
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.291 OL08-00-040010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

OL 8 must not have the rsh-server package installed.

```
GROUP ID: V-248827
RULE ID: SV-248827r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Audit:

Determine if the rsh-server package is installed with the following command:

```
$ sudo yum list installed rsh-server
```

If the rsh-server package is installed, this is a finding.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

```
$ sudo yum remove rsh-server
```


Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.292 OL08-00-040020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must cover or disable the built-in or attached camera when not in use.

```
GROUP ID: V-248828
RULE ID: SV-248828r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect from collaborative computing devices (i.e., cameras) can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

Internal Only - General

Audit:

If the device or operating system does not have a camera installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of the camera is a local AO decision.

This requirement is not applicable to dedicated VTC suites located in approved VTC locations that are centrally managed.

For an external camera, if there is not a method for the operator to manually disconnect the camera at the end of collaborative computing sessions, this is a finding.

For a built-in camera, the camera must be protected by a camera cover (e.g., laptop camera cover slide) when not in use.

If the built-in camera is not protected with a camera cover or is not physically disabled, this is a finding.

If the camera is not disconnected, covered, or physically disabled, determine if it is being disabled via software with the following commands:

Verify the operating system disables the ability to load the uvcvideo kernel module.

```
$ sudo grep -r uvcvideo /etc/modprobe.d/* | grep "/bin/false"

install uvcvideo /bin/false
```

If the command does not return any output, or the line is commented out, and the collaborative computing device has not been authorized for use, this is a finding.

Verify the camera is disabled via blacklist with the following command:

```
$ sudo grep -r uvcvideo /etc/modprobe.d/* | grep "blacklist"

blacklist uvcvideo
```

If the command does not return any output or the output is not "blacklist uvcvideo", and the collaborative computing device has not been authorized for use, this is a finding.

Remediation:

Configure OL 8 to disable the built-in or attached camera when not in use.

Build or modify the "/etc/modprobe.d/blacklist.conf" file by using the following example:

```
install uvcvideo /bin/false
blacklist uvcvideo
```

Reboot the system for the settings to take effect.

Internal Only - General

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.293 OL08-00-040021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the asynchronous transfer mode (ATM) kernel module installed if not required for operational support.

```
GROUP ID: V-248829
RULE ID: SV-248829r991589
```

Rationale:

The ATM is a transport layer protocol designed for digital transmission of multiple types of traffic, including telephony (voice), data, and video signals, in one network without the use of separate overlay networks. Disabling ATM protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the "atm" kernel module.

```
 $ sudo grep -r atm /etc/modprobe.d/* | grep -i "/bin/false" | grep -v "^#"

 install atm /bin/false
```

If the command does not return any output or the line is commented out, and use of ATM is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use ATM with the following command:

```
 $ sudo grep atm /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"

 blacklist atm
```

If the command does not return any output or the output is not "blacklist atm", and use of ATM is not documented with the ISSO as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable the ability to use the "atm" kernel module.

Create a file under "/etc/modprobe.d" with the following command:

```
$ sudo touch /etc/modprobe.d/atm.conf
```

Add the following line to the created file:

```
install atm /bin/false
```

Configure OL 8 to disable the ability to use the atm kernel module.

```
$ sudo vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist atm
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.294 OL08-00-040022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the Controller Area Network (CAN) kernel module installed if not required for operational support.

```
GROUP ID: V-248830
RULE ID: SV-248830r991589
```

Rationale:

The CAN protocol is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer. Disabling CAN protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the "can" kernel module.

```
$ sudo grep -r can /etc/modprobe.d/* | grep -i "/bin/false" | grep -v "^#"

install can /bin/false
```

If the command does not return any output or the line is commented out, and use of "can" is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use CAN with the following command:

```
$ sudo grep can /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"

blacklist can
```

If the command does not return any output or the output is not "blacklist can", and use of CAN is not documented with the ISSO as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable the ability to use the "can" kernel module.

Create a file under "/etc/modprobe.d" with the following command:

```
$ sudo touch /etc/modprobe.d/can.conf
```

Add the following line to the created file:

```
install can /bin/false
```

Configure OL 8 to disable the ability to use the can kernel module.

```
$ sudo vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist can
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.295 OL08-00-040023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the stream control transmission protocol (SCTP) kernel module installed if not required for operational support.

```
GROUP ID: V-248831
RULE ID: SV-248831r991589
```

Rationale:

The SCTP is a transport layer protocol, designed to support the idea of message-oriented communication, with several streams of messages within one connection. Disabling SCTP protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the "sctp" kernel module.

```
$ sudo grep -r sctp /etc/modprobe.d/* | grep -i "/bin/false" | grep -v "^#"

install sctp /bin/false
```

If the command does not return any output or the line is commented out, and use of SCTP is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use SCTP with the following command:

```
$ sudo grep sctp /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"

blacklist sctp
```

If the command does not return any output or the output is not "blacklist sctp", and use of SCTP is not documented with the ISSO as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to disable the ability to use the "sctp" kernel module.

Create a file under "/etc/modprobe.d" with the following command:

```
$ sudo touch /etc/modprobe.d/sctp.conf
```

Add the following line to the created file:

```
install sctp /bin/false
```

Configure OL 8 to disable the ability to use the sctp kernel module.

```
$ sudo vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist sctp
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.296 OL08-00-040024 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must disable the transparent inter-process communication (TIPC) protocol.

```
GROUP ID: V-248832
RULE ID: SV-248832r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect unused protocols can result in a system compromise.

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communications between nodes in a cluster. Disabling TIPC protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the TIPC protocol kernel module.

```
$ sudo grep -r tipc /etc/modprobe.d/* | grep "/bin/false"

install tipc /bin/false
```

If the command does not return any output, or the line is commented out, and use of the TIPC protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the TIPC protocol.

Determine if the TIPC protocol is disabled with the following command:

```
$ sudo grep -r tipc /etc/modprobe.d/* | grep "blacklist"

blacklist tipc
```

If the command does not return any output or the output is not "blacklist tipc", and use of the TIPC protocol is not documented with the ISSO as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to disable the ability to use the TIPC protocol kernel module.

Add or update the following lines in the file "/etc/modprobe.d/blacklist.conf":

```
install tipc /bin/false
blacklist tipc
```

Reboot the system for the settings to take effect.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.297 OL08-00-040025 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must disable mounting of cramfs.

```
GROUP ID: V-248833
RULE ID: SV-248833r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Removing support for unneeded filesystem types reduces the local attack surface of the server.

Compressed ROM/RAM file system (or cramfs) is a read-only file system designed for simplicity and space-efficiency. It is mainly used in embedded and small-footprint systems.

Audit:

Verify the operating system disables the ability to load the cramfs kernel module.

```
 $ sudo grep -ri cramfs /etc/modprobe.d/* | grep -i "/bin/false"

 install cramfs /bin/false
```

If the command does not return any output, or the line is commented out, and use of the cramfs protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the cramfs kernel module.

Determine if the cramfs kernel module is disabled with the following command:

```
 $ sudo grep -ri cramfs /etc/modprobe.d/* | grep -i "blacklist"

 blacklist cramfs
```

If the command does not return any output or the output is not "blacklist cramfs", and use of the cramfs kernel module is not documented with the ISSO as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to disable the ability to use the cramfs kernel module.

Add or update the following lines in the file "/etc/modprobe.d/blacklist.conf":

```
install cramfs /bin/false
blacklist cramfs
```

Reboot the system for the settings to take effect.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.298 OL08-00-040026 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must disable IEEE 1394 (FireWire) Support.

```
GROUP ID: V-248834
RULE ID: SV-248834r958478
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The IEEE 1394 (FireWire) is a serial bus standard for high-speed real-time communication. Disabling FireWire protects the system against exploitation of any flaws in its implementation.

Audit:

Verify the operating system disables the ability to load the firewire-core kernel module.

```
 $ sudo grep -ri firewire-core /etc/modprobe.d/* | grep -i "/bin/false"

 install firewire-core /bin/false
```

If the command does not return any output, or the line is commented out, and use of the firewire-core protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the firewire-core kernel module.

Determine if the firewire-core kernel module is disabled with the following command:

```
 $ sudo grep -ri firewire-core /etc/modprobe.d/* | grep -i "blacklist"

 blacklist firewire-core
```

If the command does not return any output or the output is not "blacklist firewire-core", and use of the firewire-core kernel module is not documented with the ISSO as an operational requirement, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to disable the ability to use the firewire-core kernel module.

Add or update the following lines in the file "/etc/modprobe.d/blacklist.conf":

```
install firewire-core /bin/false
blacklist firewire-core
```

Reboot the system for the settings to take effect.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Internal Only - General

1.299 OL08-00-040030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services as defined in the Ports, Protocols, and Services Management (PPSM) Category Assignments List (CAL) and vulnerability assessments.

```
GROUP ID: V-248835
RULE ID: SV-248835r958480
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality-of-life issues.

Internal Only - General

Audit:

Inspect the firewall configuration and running services to verify it is configured to prohibit or restrict the use of functions, ports, protocols, and/or services that are unnecessary or prohibited.

Check which services are currently active with the following command:

```
$ sudo firewall-cmd --list-all

custom (active)
target: DROP
icmp-block-inversion: no
interfaces: ens33
sources:
services: dhcpv6-client dns http https ldaps rpc-bind ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Ask the System Administrator for the site or program PPSM Component Local Service Assessment (CLSA). Verify the services allowed by the firewall match the PPSM CLSA.

If there are additional ports, protocols, or services that are not in the PPSM CLSA, or there are ports, protocols, or services that are prohibited by the PPSM CAL, this is a finding.

Remediation:

Update the host's firewall settings and/or running services to comply with the PPSM CLSA for the site or program and the PPSM CAL.

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

Internal Only - General

1.300 OL08-00-040070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 file system automounter must be disabled unless required.

```
GROUP ID: V-248836
RULE ID: SV-248836r958498
```

Rationale:

Verify the operating system disables the ability to automount devices.

Determine if automounter service is active with the following command:

```
$ sudo systemctl status autofs

autofs.service - Automounts filesystems on demand
Loaded: loaded (/usr/lib/systemd/system/autofs.service; disabled)
Active: inactive (dead)
```

If the "autofs" status is set to "active" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Audit:

Verify the operating system disables the ability to automount devices.

Determine if the automounter service is active with the following command:

```
$ sudo systemctl status autofs

autofs.service - Automounts filesystems on demand
Loaded: loaded (/usr/lib/systemd/system/autofs.service; disabled)
Active: inactive (dead)
```

If the "autofs" status is set to "active" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure OL 8 to disable the ability to automount devices.

Turn off the automount service with the following commands:

```
$ sudo systemctl stop autofs
$ sudo systemctl disable autofs
```

If "autofs" is required for Network File System (NFS), it must be documented with the ISSO.

Internal Only - General

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

Internal Only - General

1.301 OL08-00-040080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured to disable the ability to use USB mass storage devices.

```
GROUP ID: V-248837
RULE ID: SV-248837r986386
```

Rationale:

USB mass storage permits easy introduction of unknown devices, thereby facilitating malicious activity.

Audit:

Verify the operating system disables the ability to load the USB Storage kernel module.

```
 $ sudo grep -r usb-storage /etc/modprobe.d/* | grep -i "/bin/false"

 install usb-storage /bin/false
```

If the command does not return any output, or the line is commented out, and use of USB Storage is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Determine if USB mass storage is disabled with the following command:

```
 $ sudo grep usb-storage /etc/modprobe.d/* | grep -i "blacklist" | grep -v
"^#"

 /etc/modprobe.d/blacklist.conf:blacklist usb-storage
```

If the command does not return any output or the output is not "blacklist usb-storage" and use of USB storage devices is not documented with the ISSO as an operational requirement, this is a finding.

Remediation:

Configure OL 8 to disable the ability to use the USB Storage kernel module and to use USB mass storage devices.

```
 $ sudo vi /etc/modprobe.d/blacklist.conf
```

Add or update the lines:

```
 install usb-storage /bin/false
 blacklist usb-storage
```

Reboot the system for the settings to take effect.

Internal Only - General

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5::CM-7 (9) (b)

Internal Only - General

1.302 OL08-00-040090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

An OL 8 firewall must employ a deny-all, allow-by-exception policy for allowing connections to other systems.

```
GROUP ID: V-248839
RULE ID: SV-248839r958672
```

Rationale:

Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DoD data.

OL 8 incorporates the "firewalld" daemon, which allows for many different configurations. One of these configurations is zones. Zones can be used in a deny-all, allow-by-exception approach. The default "drop" zone will drop all incoming network packets unless it is explicitly allowed by the configuration file or is related to an outgoing network connection.

Audit:

Verify "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems with the following commands:

```
$ sudo firewall-cmd --state

running
$ sudo firewall-cmd --get-active-zones

[custom]
interfaces: ens33
$ sudo firewall-cmd --info-zone=[custom] | grep target

target: DROP
```

If no zones are active on the OL 8 interfaces or if the target is set to an option other than "DROP", this is a finding.

If the "firewalld" package is not installed, ask the System Administrator if an alternate firewall (such as iptables) is installed and in use, and how is it configured to employ a deny-all, allow-by-exception policy.

If the alternate firewall is not configured to employ a deny-all, allow-by-exception policy, this is a finding.

If no firewall is installed, this is a finding.

Internal Only - General

Remediation:

Configure the "firewalld" daemon to employ a deny-all, allow-by-exception policy with the following commands:

```
 $ sudo firewall-cmd --permanent --new-zone=[custom]

 $ sudo cp /usr/lib/firewalld/zones/drop.xml
/etc/firewalld/zones/[custom].xml
```

This will provide a clean configuration file to work with that employs a deny-all approach.

Note: Add the exceptions that are required for mission functionality and update the short title in the xml file to match the [custom] zone name.

Reload the firewall rules to make the new [custom] zone available to load:

```
 $ sudo firewall-cmd --reload
```

Set the default zone to the new [custom] zone:

```
 $ sudo firewall-cmd --set-default-zone=[custom]
```

Note: This is a runtime and permanent change.

Add any interfaces to the new [custom] zone:

```
 $ sudo firewall-cmd --permanent --zone=[custom] --change-interface=ens33
```

Reload the firewall rules for changes to take effect:

```
 $ sudo firewall-cmd --reload
```

Additional Information:

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

Internal Only - General

1.303 OL08-00-040100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A firewall must be installed on OL 8.

```
GROUP ID: V-248840
RULE ID: SV-248840r958672
```

Rationale:

"Firewalld" provides an easy and effective way to block/limit remote access to the system via ports, services, and protocols.

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

OL 8 functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that "firewalld" is installed with the following commands:

```
$ sudo yum list installed firewalld

firewalld.noarch     0.7.0-5.el8
```

If the "firewalld" package is not installed, ask the System Administrator if another firewall is installed. If no firewall is installed this is a finding.

Remediation:

Install "firewalld" with the following commands:

```
$ sudo yum install firewalld.noarch
```


Internal Only - General

Additional Information:

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

Internal Only - General

1.304 OL08-00-040101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A firewall must be active on OL 8.

```
GROUP ID: V-248841
RULE ID: SV-248841r958672
```

Rationale:

"Firewalld" provides an easy and effective way to block/limit remote access to the system via ports, services, and protocols.

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

OL 8 functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify that "firewalld" is active with the following commands:

```
$ sudo systemctl is-active firewalld

active
```

If the "firewalld" package is not "active", ask the System Administrator if another firewall is installed. If no firewall is installed and active this is a finding.

Internal Only - General

Remediation:

Configure "firewalld" to protect the operating system with the following commands:

```
$ sudo systemctl enable firewalld
$ sudo systemctl start firewalld
```

Additional Information:

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

Internal Only - General

1.305 OL08-00-040110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 wireless network adapters must be disabled.

```
GROUP ID: V-248842
RULE ID: SV-248842r991568
```

Rationale:

Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and read, altered, or used to compromise the OL 8 operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with OL 8 systems. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR keyboards, mice, and pointing devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DoD requirements for wireless data transmission and be approved for use by the Authorizing Official (AO). Although some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the OL 8 operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

Satisfies: SRG-OS-000299-GPOS-00117, SRG-OS-000300-GPOS-00118, SRG-OS-000481-GPOS-000481

Internal Only - General

Audit:

Verify there are no wireless interfaces configured on the system with the following command.

Note: This requirement is not applicable for systems that do not have physical wireless network radios.

```
$ sudo nmcli device status

DEVICE TYPE STATE CONNECTION
virbr0 bridge connected virbr0
wlp7s0 wifi connected wifiSSID
enp6s0 ethernet disconnected --
p2p-dev-wlp7s0 wifi-p2p disconnected --
lo loopback unmanaged --
virbr0-nic tun unmanaged --
```

If a wireless interface is configured and has not been documented and approved by the Information System Security Officer (ISSO), this is a finding.

Remediation:

Configure the system to disable all wireless network interfaces with the following command:

```
$ sudo nmcli radio all off
```

Additional Information:

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-001444 Protect wireless access to the system using encryption.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

Internal Only - General

1.306 OL08-00-040111 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 Bluetooth must be disabled.

```
GROUP ID: V-248843
RULE ID: SV-248843r991569
```

Rationale:

Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and read, altered, or used to compromise the OL 8 operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with OL 8 systems. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR keyboards, mice, and pointing devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DoD requirements for wireless data transmission and be approved for use by the Authorizing Official (AO). Although some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the OL 8 operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

Internal Only - General

Audit:

If the device or operating system does not have a Bluetooth adapter installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of Bluetooth is a local AO decision.

Determine if Bluetooth is disabled with the following command:

```
$ sudo grep -r bluetooth /etc/modprobe.d

/etc/modprobe.d/bluetooth.conf:install bluetooth /bin/false
```

If the command does not return any output or the line is commented out and the collaborative computing device has not been authorized for use, this is a finding.

Verify the operating system disables the ability to use Bluetooth with the following command:

```
$ sudo grep -r bluetooth /etc/modprobe.d | grep -i "blacklist" | grep -v
"^#"

blacklist bluetooth
```

If the command does not return any output or the output is not "blacklist bluetooth", and use of Bluetooth is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the Bluetooth adapter when not in use.

Build or modify the "/etc/modprobe.d/bluetooth.conf" file with the following line:

```
install bluetooth /bin/false
```

Disable the ability to use the Bluetooth kernel module.

```
$ sudo vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist bluetooth
```

Reboot the system for the settings to take effect.

Internal Only - General

Additional Information:

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-001444 Protect wireless access to the system using encryption.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

Internal Only - General

1.307 OL08-00-040120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/dev/shm" with the "nodev" option.

```
GROUP ID: V-248844
RULE ID: SV-248844r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/dev/shm" is mounted with the "nodev" option:

```
$ sudo mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for "/dev/shm":

```
$ sudo cat /etc/fstab | grep /dev/shm

tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nodev" option is missing, or if "/dev/shm" is mounted without the "nodev" option, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 so that "/dev/shm" is mounted with the "nodev" option by adding/modifying "/etc/fstab" with the following line:

```
tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.308 OL08-00-040121 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/dev/shm" with the "nosuid" option.

```
GROUP ID: V-248845
RULE ID: SV-248845r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/dev/shm" is mounted with the "nosuid" option:

```
$ sudo mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for "/dev/shm":

```
$ sudo cat /etc/fstab | grep /dev/shm

tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nosuid" option is missing, or if "/dev/shm" is mounted without the "nosuid" option, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 so that "/dev/shm" is mounted with the "nosuid" option by adding/modifying "/etc/fstab" with the following line:

```
tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.309 OL08-00-040122 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/dev/shm" with the "noexec" option.

```
GROUP ID: V-248846
RULE ID: SV-248846r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/dev/shm" is mounted with the "noexec" option:

```
$ sudo mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for "/dev/shm":

```
$ sudo cat /etc/fstab | grep /dev/shm

tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "noexec" option is missing, or if "/dev/shm" is mounted without the "noexec" option, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 so that "/dev/shm" is mounted with the "noexec" option by adding/modifying "/etc/fstab" with the following line:

```
tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.310 OL08-00-040123 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/tmp" with the "nodev" option.

```
GROUP ID: V-248847
RULE ID: SV-248847r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/tmp" is mounted with the "nodev" option:

```
$ sudo mount | grep /tmp

/dev/mapper/ol-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for /tmp:

```
$ sudo cat /etc/fstab | grep /tmp

/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nodev" option is missing, or if /tmp is mounted without the "nodev" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /tmp is mounted with the "nodev" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.311 OL08-00-040124 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/tmp" with the "nosuid" option.

```
GROUP ID: V-248848
RULE ID: SV-248848r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/tmp" is mounted with the "nosuid" option:

```
$ sudo mount | grep /tmp

/dev/mapper/ol-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for /tmp:

```
$ sudo cat /etc/fstab | grep /tmp

/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nosuid" option is missing, or if /tmp is mounted without the "nosuid" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /tmp is mounted with the "nosuid" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.312 OL08-00-040125 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/tmp" with the "noexec" option.

```
GROUP ID: V-248849
RULE ID: SV-248849r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/tmp" is mounted with the "noexec" option:

```
$ sudo mount | grep /tmp

/dev/mapper/ol-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for /tmp:

```
$ sudo cat /etc/fstab | grep /tmp

/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "noexec" option is missing, or if /tmp is mounted without the "noexec" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /tmp is mounted with the "noexec" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-tmp /tmp xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.313 OL08-00-040126 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/log" with the "nodev" option.

```
GROUP ID: V-248850
RULE ID: SV-248850r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "nodev" option:

```
$ sudo mount | grep /var/log

/dev/mapper/ol-var_log on /var/log type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for /var/log:

```
$ sudo cat /etc/fstab | grep /var/log

/dev/mapper/ol-var_log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nodev" option is missing, or if /var/log is mounted without the "nodev" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /var/log is mounted with the "nodev" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.314 OL08-00-040127 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/log" with the "nosuid" option.

```
GROUP ID: V-248851
RULE ID: SV-248851r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "nosuid" option:

```
$ sudo mount | grep /var/log

/dev/mapper/ol-var_log on /var/log type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for /var/log:

```
$ sudo cat /etc/fstab | grep /var/log

/dev/mapper/ol-var_log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nosuid" option is missing, or if /var/log is mounted without the "nosuid" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /var/log is mounted with the "nosuid" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.315 OL08-00-040128 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/log" with the "noexec" option.

```
GROUP ID: V-248852
RULE ID: SV-248852r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "noexec" option:

```
$ sudo mount | grep /var/log

/dev/mapper/ol-var_log on /var/log type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for /var/log:

```
$ sudo cat /etc/fstab | grep /var/log

/dev/mapper/ol-var_log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "noexec" option is missing, or if /var/log is mounted without the "noexec" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /var/log is mounted with the "noexec" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_log /var/log xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.316 OL08-00-040129 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/log/audit" with the "nodev" option.

```
GROUP ID: V-248853
RULE ID: SV-248853r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Internal Only - General

Audit:

Verify "/var/log/audit" is mounted with the "nodev" option:

```
$ sudo mount | grep /var/log/audit

/dev/mapper/ol-var_log_audit on /var/log/audit type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for /var/log/audit:

```
$ sudo cat /etc/fstab | grep /var/log/audit

/dev/mapper/ol-var_log_audit /var/log/audit xfs defaults,nodev,nosuid,noexec
0 0
```

If results are returned and the "nodev" option is missing, or if /var/log/audit is mounted without the "nodev" option, this is a finding.

Remediation:

Configure the system so that /var/log/audit is mounted with the "nodev" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_log_audit /var/log/audit xfs defaults,nodev,nosuid,noexec
0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.317 OL08-00-040130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/log/audit" with the "nosuid" option.

```
GROUP ID: V-248854
RULE ID: SV-248854r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Internal Only - General

Audit:

Verify "/var/log/audit" is mounted with the "nosuid" option:

```
$ sudo mount | grep /var/log/audit

/dev/mapper/ol-var_log_audit on /var/log/audit type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for /var/log/audit:

```
$ sudo cat /etc/fstab | grep /var/log/audit

/dev/mapper/ol-var_log_audit /var/log/audit xfs defaults,nodev,nosuid,noexec
0 0
```

If results are returned and the "nosuid" option is missing, or if /var/log/audit is mounted without the "nosuid" option, this is a finding.

Remediation:

Configure the system so that /var/log/audit is mounted with the "nosuid" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_log_audit /var/log/audit xfs defaults,nodev,nosuid,noexec
0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.318 OL08-00-040131 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/log/audit" with the "noexec" option.

```
GROUP ID: V-248855
RULE ID: SV-248855r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Internal Only - General

Audit:

Verify "/var/log/audit" is mounted with the "noexec" option:

```
$ sudo mount | grep /var/log/audit

/dev/mapper/ol-var_log_audit on /var/log/audit type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for /var/log/audit:

```
$ sudo cat /etc/fstab | grep /var/log/audit

/dev/mapper/ol-var_log_audit /var/log/audit xfs defaults,nodev,nosuid,noexec
0 0
```

If results are returned and the "noexec" option is missing, or if /var/log/audit is mounted without the "noexec" option, this is a finding.

Remediation:

Configure the system so that /var/log/audit is mounted with the "noexec" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_log_audit /var/log/audit xfs defaults,nodev,nosuid,noexec
0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.319 OL08-00-040132 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/tmp" with the "nodev" option.

```
GROUP ID: V-248856
RULE ID: SV-248856r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/tmp" is mounted with the "nodev" option:

```
$ sudo mount | grep /var/tmp

/dev/mapper/ol-var_tmp on /var/tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nodev" option is configured for /var/tmp:

```
$ sudo cat /etc/fstab | grep /var/tmp

/dev/mapper/ol-var_tmp /var/tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nodev" option is missing, or if /var/tmp is mounted without the "nodev" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /var/tmp is mounted with the "nodev" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_tmp /var/tmp xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.320 OL08-00-040133 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/tmp" with the "nosuid" option.

```
GROUP ID: V-248857
RULE ID: SV-248857r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/tmp" is mounted with the "nosuid" option:

```
$ sudo mount | grep /var/tmp

/dev/mapper/ol-var_tmp on /var/tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "nosuid" option is configured for /var/tmp:

```
$ sudo cat /etc/fstab | grep /var/tmp

/dev/mapper/ol-var_tmp /var/tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "nosuid" option is missing, or if /var/tmp is mounted without the "nosuid" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /var/tmp is mounted with the "nosuid" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_tmp /var/tmp xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.321 OL08-00-040134 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must mount "/var/tmp" with the "noexec" option.

```
GROUP ID: V-248858
RULE ID: SV-248858r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/tmp" is mounted with the "noexec" option:

```
$ sudo mount | grep /var/tmp

/dev/mapper/ol-var_tmp on /var/tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

Verify that the "noexec" option is configured for /var/tmp:

```
$ sudo cat /etc/fstab | grep /var/tmp

/dev/mapper/ol-var_tmp /var/tmp xfs defaults,nodev,nosuid,noexec 0 0
```

If results are returned and the "noexec" option is missing, or if /var/tmp is mounted without the "noexec" option, this is a finding.

Internal Only - General

Remediation:

Configure the system so that /var/tmp is mounted with the "noexec" option by adding /modifying the /etc/fstab with the following line:

```
/dev/mapper/ol-var_tmp /var/tmp xfs defaults,nodev,nosuid,noexec 0 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

Internal Only - General

1.322 OL08-00-040135 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "fapolicy" module must be installed.

```
GROUP ID: V-248859
RULE ID: SV-248859r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Using a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

Users' home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with a System Administrator through shared resources.

OL 8 ships with many optional packages. One such package is a file access policy daemon called "fapolicyd". This is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155

Audit:

Verify the OL 8 "fapolicyd" is installed.

Check that "fapolicyd" is installed with the following command:

```
$ sudo yum list installed fapolicyd

Installed Packages
fapolicyd.x86_64
```

If "fapolicyd" is not installed, this is a finding.

Internal Only - General

Remediation:

Install "fapolicyd" with the following command:

```
$ sudo yum install fapolicyd.x86_64
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4::CM-7 (5) (b)
- NIST SP 800-53 Revision 5::CM-7 (5) (b)

Internal Only - General

1.323 OL08-00-040136 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 "fapolicy" module must be enabled.

```
GROUP ID: V-248860
RULE ID: SV-248860r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Using a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

Users' home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with a System Administrator through shared resources.

OL 8 ships with many optional packages. One such package is a file access policy daemon called "fapolicyd". This is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155

Audit:

Verify the OL 8 "fapolicyd" is enabled and running with the following command:

```
$ sudo systemctl status fapolicyd.service

fapolicyd.service - File Access Policy Daemon
Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor
preset: disabled)
Active: active (running)
```

If fapolicyd is not enabled and running, this is a finding.

Internal Only - General

Remediation:

Enable "fapolicyd" using the following command:

```
$ sudo systemctl enable --now fapolicyd
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4::CM-7 (5) (b)
- NIST SP 800-53 Revision 5::CM-7 (5) (b)

Internal Only - General

1.324 OL08-00-040137 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 fapolicy module must be configured to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

```
GROUP ID: V-248861
RULE ID: SV-248861r958804
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Using a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

Users' home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with a System Administrator through shared resources.

OL 8 ships with many optional packages. One such package is a file access policy daemon called "fapolicyd". This is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155

Internal Only - General

Audit:

Verify the OL 8 "fapolicyd" employs a deny-all, permit-by-exception policy.

Check that "fapolicyd" is in enforcement mode with the following command:

```
$ sudo grep permissive /etc/fapolicyd/fapolicyd.conf

permissive = 0
```

Check that fapolicyd employs a deny-all policy on system mounts with the following commands:

For OL 8.4 systems and older:

```
$ sudo tail /etc/fapolicyd/fapolicyd.rules
```

For OL 8.5 systems and newer:

```
$ sudo tail /etc/fapolicyd/compiled.rules

allow exe=/usr/bin/python3.7 : ftype=text/x-python
deny_audit perm=any pattern=ld_so : all
deny perm=any all : all
```

If fapolicyd is not running in enforcement mode with a deny-all, permit-by-exception policy, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to employ a deny-all, permit-by-exception application whitelisting policy with "fapolicyd".

With the "fapolicyd" installed and enabled, configure the daemon to function in permissive mode until the whitelist is built correctly to avoid system lockout. Do this by editing the "/etc/fapolicyd/fapolicyd.conf" file with the following line:

```
permissive = 1
```

For OL 8.4 systems and older:

Build the whitelist in the "/etc/fapolicyd/fapolicyd.rules" file ensuring the last rule is

```
deny perm=any all : all
```

For OL 8.5 systems and newer:

Build the whitelist in a file within the "/etc/fapolicyd/rules.d" directory ensuring the last rule is

```
deny perm=any all : all
```

Once it is determined the whitelist is built correctly, set the fapolicyd to enforcing mode by editing the "permissive" line in the /etc/fapolicyd/fapolicyd.conf file.

```
permissive = 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4::CM-7 (5) (b)
- NIST SP 800-53 Revision 5::CM-7 (5) (b)

Internal Only - General

1.325 OL08-00-040139 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must have the USBGuard installed.

```
GROUP ID: V-248862
RULE ID: SV-248862r986387
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include but are not limited to such devices as flash drives, external storage, and printers.

A new feature that OL 8 provides is the USBGuard software framework. The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbguard-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the "usbguard" tool.

The system administrator (SA) must work with the site information system security officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

Audit:

Verify USBGuard is installed on the operating system with the following command:

```
$ sudo yum list installed usbguard

Installed Packages
usbguard.x86_64                    0.7.8-7.el8             @ol8_appstream
```

If the USBGuard package is not installed, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Internal Only - General

Remediation:

Install the USBGuard package with the following command:

```
$ sudo yum install usbguard.x86_64
```

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5::CM-7 (9) (b)

Internal Only - General

1.326 OL08-00-040140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must block unauthorized peripherals before establishing a connection.

```
GROUP ID: V-248863
RULE ID: SV-248863r958820
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include but are not limited to such devices as flash drives, external storage, and printers.

A new feature that OL 8 provides is the USBGuard software framework. The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbguard-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the "usbguard" tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

Audit:

Verify the USBGuard has a policy configured with the following command:

```
$ sudo usbguard list-rules
```

If the command does not return results or an error is returned, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to enable the blocking of unauthorized peripherals with the following command:

This command must be run from a root shell and will create an allow list for any usb devices currently connect to the system.

```
# usbguard generate-policy > /etc/usbguard/rules.conf
```

Note: Enabling and starting usbguard without properly configuring it for an individual system will immediately prevent any access over a usb device such as a keyboard or mouse.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

Internal Only - General

1.327 OL08-00-040141 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable the USBGuard.

```
GROUP ID: V-248864
RULE ID: SV-248864r986388
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include but are not limited to such devices as flash drives, external storage, and printers.

A new feature that OL 8 provides is the USBGuard software framework. The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbguard-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the "usbguard" tool.

The system administrator (SA) must work with the site information system security officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

Audit:

Verify the operating system has enabled the use of the USBGuard with the following command:

```
$ sudo systemctl status usbguard.service

usbguard.service - USBGuard daemon
Loaded: loaded (/usr/lib/systemd/system/usbguard.service; enabled; vendor
preset: disabled)
Active: active (running)
```

If the usbguard.service is not enabled and active, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Internal Only - General

Remediation:

Configure the operating system to enable the blocking of unauthorized peripherals with the following commands:

```
$ sudo systemctl enable usbguard.service
$ sudo systemctl start usbguard.service
```

Note: Enabling and starting usbguard without properly configuring it for an individual system will immediately prevent any access over a usb device such as a keyboard or mouse.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5::CM-7 (9) (b)

Internal Only - General

1.328 OL08-00-040150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A firewall must be able to protect against or limit the effects of denial-of-service (DoS) attacks by ensuring OL 8 can implement rate-limiting measures on impacted network interfaces.

```
GROUP ID: V-248865
RULE ID: SV-248865r958528
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of OL 8 to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exists to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Since version 0.6.0, "firewalld" has incorporated "nftables" as its backend support. Using the limit statement in "nftables" can help to mitigate DoS attacks.

Satisfies: SRG-OS-000142-GPOS-00071, SRG-OS-000298-GPOS-00116, SRG-OS-000420-GPOS-00186

Audit:

Verify "nftables" is configured to allow rate limits on any connection to the system with the following command.

Verify "firewalld" has "nftables" set as the default backend:

```
$ sudo grep -i firewallbackend /etc/firewalld/firewalld.conf

# FirewallBackend
FirewallBackend=nftables
```

If the "nftables" is not set as the "firewallbackend" default, this is a finding.

Internal Only - General

Remediation:

Configure "nftables" to be the default "firewallbackend" for "firewalld" by adding or editing the following line in "/etc/firewalld/firewalld.conf":

```
FirewallBackend=nftables
```

Establish rate-limiting rules based on organization-defined types of DoS attacks on impacted network interfaces.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

CCI-002322 Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

- NIST SP 800-53 Revision 4::AC-17 (9)
- NIST SP 800-53 Revision 5::AC-17 (9)

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

Internal Only - General

1.329 OL08-00-040159 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 networked systems must have SSH installed.

```
GROUP ID: V-248866
RULE ID: SV-248866r958908
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify SSH is installed with the following command:

```
$ sudo yum list installed openssh-server

openssh-server.x86_64                 8.0p1-5.el8          @anaconda
```

If the "SSH server" package is not installed, this is a finding.

Remediation:

Install SSH packages onto the host with the following command:

```
$ sudo yum install openssh-server.x86_64
```


Internal Only - General

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

Internal Only - General

1.330 OL08-00-040160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All OL 8 networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

```
GROUP ID: V-248867
RULE ID: SV-248867r958908
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify SSH is loaded and active with the following command:

```
$ sudo systemctl status sshd

sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)
Active: active (running) since Tue 2015-11-17 15:17:22 EST; 4 weeks 0 days
ago
Main PID: 1348 (sshd)
CGroup: /system.slice/sshd.service
1053 /usr/sbin/sshd -D
```

If "sshd" does not show a status of "active" and "running", this is a finding.

Internal Only - General

Remediation:

Configure the SSH service to automatically start after reboot with the following command:

```
$ sudo systemctl enable sshd.service
```

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

Internal Only - General

1.331 OL08-00-040161 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must force a frequent session key renegotiation for SSH connections to the server.

```
GROUP ID: V-248868
RULE ID: SV-248868r958408
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DOD data may be compromised.

Session key regeneration limits the chances of a session key becoming compromised.

Audit:

Verify the SSH server is configured to force frequent session key renegotiation with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*rekeylimit'

RekeyLimit 1G 1h
```

If "RekeyLimit" does not have a maximum data amount and maximum time defined or is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system to force a frequent session key renegotiation for SSH connections to the server by adding or modifying the following line in the "/etc/ssh/sshd_config" file:

```
RekeyLimit 1G 1h
```

The SSH daemon must be restarted for the settings to take effect.

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Internal Only - General

1.332 OL08-00-040170 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The x86 Ctrl-Alt-Delete key sequence must be disabled on OL 8.

```
GROUP ID: V-248869
RULE ID: SV-248869r991589
```

Rationale:

A locally logged-on user, who presses Ctrl-Alt-Delete when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of system availability due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify OL 8 is not configured to reboot the system when Ctrl-Alt-Delete is pressed with the following command:

```
$ sudo systemctl status ctrl-alt-del.target | grep Loaded:

Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)
```

If the "ctrl-alt-del.target" Loaded: value is not set to "masked", this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the command line with the following commands:

```
$ sudo systemctl disable ctrl-alt-del.target
$ sudo systemctl mask ctrl-alt-del.target

Created symlink /etc/systemd/system/ctrl-alt-del.target -> /dev/null
```

Reload the daemon to take effect:

```
$ sudo systemctl daemon-reload
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.333 OL08-00-040171 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The x86 Ctrl-Alt-Delete key sequence in OL 8 must be disabled if a graphical user interface is installed.

```
GROUP ID: V-248870
RULE ID: SV-248870r991589
```

Rationale:

A locally logged-on user, who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify OL 8 is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface with the following command:

```
$ sudo grep logout /etc/dconf/db/local.d/*

logout=''
```

If the "logout" key is bound to an action, is commented out, or is missing, this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence when using a graphical user interface by creating or editing the "/etc/dconf/db/local.d/00-disable-CAD" file.

Add the setting to disable the Ctrl-Alt-Delete sequence for a graphical user interface:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=''
```

Update the dconf settings:

```
$ sudo dconf update
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.334 OL08-00-040172 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable the systemd Ctrl-Alt-Delete burst key sequence.

```
GROUP ID: V-248871
RULE ID: SV-248871r991589
```

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete when at the console can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify OL 8 is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds with the following command:

```
$ sudo grep -i ctrl /etc/systemd/system.conf

CtrlAltDelBurstAction=none
```

If the "CtrlAltDelBurstAction" is not set to "none" or is commented out or missing, this is a finding.

Remediation:

Configure the system to disable the CtrlAltDelBurstAction by added or modifying the following line in the "/etc/systemd/system.conf" configuration file:

```
CtrlAltDelBurstAction=none
```

Reload the daemon for this change to take effect:

```
$ sudo systemctl daemon-reload
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.335 OL08-00-040180 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

OL 8 must disable the debug-shell systemd service.

```
GROUP ID: V-248872
RULE ID: SV-248872r991589
```

Rationale:

The debug-shell requires no authentication and provides root privileges to anyone who has physical access to the machine. While this feature is disabled by default, masking it adds a layer of assurance that it will not be enabled via a dependency in "system". This also prevents attackers with physical access from trivially bypassing security on the machine through valid troubleshooting configurations and gaining root access when the system is rebooted.

Audit:

Verify OL 8 is configured to mask the "debug-shell systemd" service with the following command:

```
$ sudo systemctl status debug-shell.service

debug-shell.service
Loaded: masked (Reason: Unit debug-shell.service is masked.)
Active: inactive (dead)
```

If the "debug-shell.service" is loaded and not masked, this is a finding.

Remediation:

Configure the system to mask the "debug-shell systemd" service with the following command:

```
$ sudo systemctl mask debug-shell.service

Created symlink /etc/systemd/system/debug-shell.service -> /dev/null
```

Reload the daemon to take effect:

```
$ sudo systemctl daemon-reload
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.336 OL08-00-040190 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for OL 8 operational support.

```
GROUP ID: V-248873
RULE ID: SV-248873r991589
```

Rationale:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Audit:

Verify a TFTP server has not been installed on the system with the following command:

```
$ sudo yum list installed tftp-server

tftp-server.x86_64 5.2-24.el8
```

If TFTP is installed and the requirement for TFTP is not documented with the ISSO, this is a finding.

Remediation:

Remove the TFTP package from the system with the following command:

```
$ sudo yum remove tftp-server
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.337 OL08-00-040200 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The root account must be the only account having unrestricted access to the OL 8 system.

```
GROUP ID: V-248874
RULE ID: SV-248874r991589
```

Rationale:

If an account other than root also has a User Identifier (UID) of "0", it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of "0" afford an opportunity for potential intruders to guess a password for a privileged account.

Audit:

Check the system for duplicate UID "0" assignments with the following command:

```
$ sudo awk -F: '$3 == 0 {print $1}' /etc/passwd
```

If any accounts other than root have a UID of "0", this is a finding.

Remediation:

Change the UID of any account on the system, other than root, that has a UID of "0".

If the account is associated with system commands or applications, change the UID to one greater than "0" but less than "1000". Otherwise, assign a UID of greater than "1000" that has not already been assigned.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.338 OL08-00-040209 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-248875
RULE ID: SV-248875r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 will not accept IPv4 ICMP redirect messages.

Check the value of the default "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.default.accept_redirects

net.ipv4.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.default.accept_redirects /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.default.accept_redirects = 0
```

If "net.ipv4.conf.default.accept_redirects" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to prevent IPv4 ICMP redirect messages from being accepted with the following command:

```
$ sudo sysctl -w net.ipv4.conf.default.accept_redirects=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.default.accept_redirects=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.339 OL08-00-040210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-248876
RULE ID: SV-248876r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 will not accept IPv6 ICMP redirect messages.

Note: IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the default "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv6.conf.default.accept_redirects

net.ipv6.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.default.accept_redirects /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.default.accept_redirects = 0
```

If "net.ipv6.conf.default.accept_redirects" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to prevent IPv6 ICMP redirect messages from being accepted with the following command:

```
$ sudo sysctl -w net.ipv6.conf.default.accept_redirects=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.conf" or in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.default.accept_redirects=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.340 OL08-00-040220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not send Internet Control Message Protocol (ICMP) redirects.

```
GROUP ID: V-248877
RULE ID: SV-248877r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

There are notable differences between Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). There is only a directive to disable sending of IPv4 redirected packets. Refer to RFC4294 for an explanation of "IPv6 Node Requirements", which resulted in this difference between IPv4 and IPv6.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not send IPv4 ICMP redirect messages.

Check the value of the "all send_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.all.send_redirects

net.ipv4.conf.all.send_redirects = 0
```

If the returned line does not have a value of "0" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.all.send_redirects /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.all.send_redirects = 0
```

If "net.ipv4.conf.all.send_redirects" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not allow interfaces to perform IPv4 ICMP redirects with the following command:

```
$ sudo sysctl -w net.ipv4.conf.all.send_redirects=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.conf" or in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.all.send_redirects=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.341 OL08-00-040230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not respond to Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

```
GROUP ID: V-248878
RULE ID: SV-248878r991589
```

Rationale:

Responding to broadcast ICMP echoes facilitates network mapping and provides a vector for amplification attacks.

There are notable differences between Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 does not implement the same method of broadcast as IPv4. Instead, IPv6 uses multicast addressing to the all-hosts multicast group. Refer to RFC4294 for an explanation of "IPv6 Node Requirements", which resulted in this difference between IPv4 and IPv6.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not respond to ICMP echoes sent to a broadcast address.

Check the value of the "icmp_echo_ignore_broadcasts" variable with the following command:

```
$ sudo sysctl net.ipv4.icmp_echo_ignore_broadcasts

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

If the returned line does not have a value of "1", a line is not returned, or the retuned line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.icmp_echo_ignore_broadcasts /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.icmp_echo_ignore_broadcasts = 1
```

If "net.ipv4.icmp_echo_ignore_broadcasts" is not set to "1", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not respond to IPv4 ICMP echoes sent to a broadcast address with the following command:

```
$ sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "1" is not the system's default value, add or update the following line in "/etc/sysctl.conf" or in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.icmp_echo_ignore_broadcasts=1
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.342 OL08-00-040239 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not forward IPv4 source-routed packets.

```
GROUP ID: V-248879
RULE ID: SV-248879r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not accept IPv4 source-routed packets.

Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv4.conf.all.accept_source_route

net.ipv4.conf.all.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.all.accept_source_route /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.all.accept_source_route = 0
```

If "net.ipv4.conf.all.accept_source_route" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not forward IPv4 source-routed packets with the following command:

```
$ sudo sysctl -w net.ipv4.conf.all.accept_source_route=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's all value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.all.accept_source_route=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.343 OL08-00-040240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not forward IPv6 source-routed packets.

```
GROUP ID: V-248880
RULE ID: SV-248880r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not accept IPv6 source-routed packets.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv6.conf.all.accept_source_route

net.ipv6.conf.all.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.all.accept_source_route /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.all.accept_source_route = 0
```

If "net.ipv6.conf.all.accept_source_route" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not forward IPv6 source-routed packets with the following command:

```
$ sudo sysctl -w net.ipv6.conf.all.accept_source_route=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's all value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.accept_source_route=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.344 OL08-00-040249 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not forward IPv4 source-routed packets by default.

```
GROUP ID: V-248881
RULE ID: SV-248881r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not accept IPv4 source-routed packets by default.

Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv4.conf.default.accept_source_route

net.ipv4.conf.default.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.default.accept_source_route /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.default.accept_source_route = 0
```

If "net.ipv4.conf.default.accept_source_route" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not forward IPv4 source-routed packets by default with the following command:

```
$ sudo sysctl -w net.ipv4.conf.default.accept_source_route=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.default.accept_source_route=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.345 OL08-00-040250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not forward IPv6 source-routed packets by default.

```
GROUP ID: V-248882
RULE ID: SV-248882r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not accept IPv6 source-routed packets by default.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv6.conf.default.accept_source_route

net.ipv6.conf.default.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.default.accept_source_route /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.default.accept_source_route = 0
```

If "net.ipv6.conf.default.accept_source_route" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not forward IPv6 source-routed packets by default with the following command:

```
$ sudo sysctl -w net.ipv6.conf.default.accept_source_route=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.default.accept_source_route=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.346 OL08-00-040259 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not enable IPv4 packet forwarding unless the system is a router.

```
GROUP ID: V-252662
RULE ID: SV-252662r991589
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify OL 8 is not performing IPv4 packet forwarding, unless the system is a router.

Check that IPv4 forwarding is disabled using the following command:

```
$ sudo sysctl net.ipv4.conf.all.forwarding

net.ipv4.conf.all.forwarding = 0
```

If the IPv4 forwarding value is not "0" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Check that the configuration files are present to enable this network parameter:

```
$ sudo grep -r net.ipv4.conf.all.forwarding /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.all.forwarding = 0
```

If "net.ipv4.conf.all.forwarding" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to not allow IPv4 packet forwarding unless the system is a router.

Add or edit the following line in a system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.forwarding=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.347 OL08-00-040260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not enable IPv6 packet forwarding unless the system is a router.

```
GROUP ID: V-248883
RULE ID: SV-248883r991589
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 is not performing IPv6 packet forwarding unless the system is a router.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Determine if IPv6 forwarding is disabled using the following commands:

```
$ sudo sysctl net.ipv6.conf.all.forwarding

net.ipv6.conf.all.forwarding = 0
```

If the IPv6 forwarding value is "1" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.all.forwarding /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.all.forwarding = 0
```

If "net.ipv6.conf.all.forwarding" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not allow IPv6 packet forwarding unless the system is a router with the following command:

```
$ sudo sysctl -w net.ipv6.conf.all.forwarding=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value, add or update the following lines in "/etc/sysctl.conf" or in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.forwarding=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.348 OL08-00-040261 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not accept router advertisements on all IPv6 interfaces.

```
GROUP ID: V-248884
RULE ID: SV-248884r991589
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

An illicit router advertisement message could result in a man-in-the-middle attack.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not accept router advertisements on all IPv6 interfaces unless the system is a router.

Note: If IPv6 is disabled on the system, this requirement is not applicable.

Determine if router advertisements are not accepted by using the following command:

```
$ sudo sysctl net.ipv6.conf.all.accept_ra

net.ipv6.conf.all.accept_ra = 0
```

If the "accept_ra" value is not "0" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.all.accept_ra /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.all.accept_ra = 0
```

If "net.ipv6.conf.all.accept_ra" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system to not accept router advertisements on all IPv6 interfaces unless the system is a router with the following commands:

```
$ sudo sysctl -w net.ipv6.conf.all.accept_ra=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value, add or update the following lines in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.accept_ra=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.349 OL08-00-040262 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not accept router advertisements on all IPv6 interfaces by default.

```
GROUP ID: V-248885
RULE ID: SV-248885r991589
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

An illicit router advertisement message could result in a man-in-the-middle attack.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not accept router advertisements on all IPv6 interfaces by default, unless the system is a router.

Note: If IPv6 is disabled on the system, this requirement is not applicable.

Determine if router advertisements are not accepted by using the following command:

```
$ sudo sysctl net.ipv6.conf.default.accept_ra

net.ipv6.conf.default.accept_ra = 0
```

If the "accept_ra" value is not "0" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.default.accept_ra /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.default.accept_ra = 0
```

If "net.ipv6.conf.default.accept_ra" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system to not accept router advertisements on all IPv6 interfaces by default, unless the system is a router, with the following commands:

```
$ sudo sysctl -w net.ipv6.conf.default.accept_ra=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value, add or update the following lines in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.default.accept_ra=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.350 OL08-00-040270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not allow interfaces to perform Internet Control Message Protocol (ICMP) redirects by default.

```
GROUP ID: V-248886
RULE ID: SV-248886r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table, possibly revealing portions of the network topology.

There are notable differences between Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). There is only a directive to disable sending of IPv4 redirected packets. Refer to RFC4294 for an explanation of "IPv6 Node Requirements", which resulted in this difference between IPv4 and IPv6.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 does not allow interfaces to perform Internet Protocol version 4 (IPv4) ICMP redirects by default.

Check the value of the "default send_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.default.send_redirects

net.ipv4.conf.default.send_redirects=0
```

If the returned line does not have a value of "0" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.default.send_redirects /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.default.send_redirects = 0
```

If "net.ipv4.conf.default.send_redirects" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to not allow interfaces to perform Internet Protocol version 4 (IPv4) ICMP redirects by default with the following command:

```
$ sudo sysctl -w net.ipv4.conf.default.send_redirects=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.conf" or in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.default.send_redirects=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.351 OL08-00-040279 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.

```
GROUP ID: V-248887
RULE ID: SV-248887r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify OL 8 ignores IPv4 ICMP redirect messages.

Check the value of the "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.all.accept_redirects

net.ipv4.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.all.accept_redirects /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.all.accept_redirects = 0
```

If "net.ipv4.conf.all.accept_redirects" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to ignore IPv4 ICMP redirect messages with the following command:

```
$ sudo sysctl -w net.ipv4.conf.all.accept_redirects=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv4.conf.all.accept_redirects = 0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.352 OL08-00-040280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.

```
GROUP ID: V-248888
RULE ID: SV-248888r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 ignores IPv6 ICMP redirect messages.

Note: If IPv6 is disabled on the system, this requirement is Not Applicable.

Check the value of the "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv6.conf.all.accept_redirects

net.ipv6.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv6.conf.all.accept_redirects /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv6.conf.all.accept_redirects = 0
```

If "net.ipv6.conf.all.accept_redirects" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to ignore IPv6 ICMP redirect messages with the following command:

```
$ sudo sysctl -w net.ipv6.conf.all.accept_redirects=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

If "0" is not the system's default value then add or update the following line in the appropriate file under "/etc/sysctl.d":

```
net.ipv6.conf.all.accept_redirects = 0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.353 OL08-00-040281 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable access to the network "bpf" syscall from unprivileged processes.

```
GROUP ID: V-248889
RULE ID: SV-248889r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify OL 8 prevents privilege escalation through the kernel by disabling access to the "bpf" syscall with the following commands:

```
$ sudo sysctl kernel.unprivileged_bpf_disabled

kernel.unprivileged_bpf_disabled = 1
```

If the returned line does not have a value of "1" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r kernel.unprivileged_bpf_disabled /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: kernel.unprivileged_bpf_disabled = 1
```

If "kernel.unprivileged_bpf_disabled" is not set to "1", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure the system to prevent privilege escalation through the kernel by disabling access to the "bpf" syscall by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.unprivileged_bpf_disabled = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.354 OL08-00-040282 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must restrict the use of "ptrace" to descendant processes.

```
GROUP ID: V-248890
RULE ID: SV-248890r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify OL 8 restricts the use of "ptrace" to descendant processes with the following commands:

```
$ sudo sysctl kernel.yama.ptrace_scope

kernel.yama.ptrace_scope = 1
```

If the returned line does not have a value of "1" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r kernel.yama.ptrace_scope /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: kernel.yama.ptrace_scope = 1
```

If "kernel.yama.ptrace_scope" is not set to "1", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure the system to restrict the use of "ptrace" to descendant processes by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.yama.ptrace_scope = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.355 OL08-00-040283 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must restrict exposed kernel pointer addresses access.

```
GROUP ID: V-248891
RULE ID: SV-248891r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Audit:

Verify OL 8 restricts exposed kernel pointer addresses access with the following commands:

```
$ sudo sysctl kernel.kptr_restrict

kernel.kptr_restrict = 1
```

If the returned line does not have a value of "1" or "2" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r kernel.kptr_restrict /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: kernel.kptr_restrict = 1
```

If "kernel.kptr_restrict" is not set to "1" or "2", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Configure the system to restrict exposed kernel pointer addresses access by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.kptr_restrict = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.356 OL08-00-040284 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must disable the use of user namespaces.

```
GROUP ID: V-248892
RULE ID: SV-248892r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

User namespaces are used primarily for Linux containers. "Rootful" containers run with root privileges on the host system and may pose a security risk if compromised. "Rootless" containers run without root privileges and allow for better isolation from the host system. The value "0" disallows the use of user namespaces. When containers are not in use, namespaces should be disallowed. When privileged user namespaces or "rootful" containers are in use, user namespaces should be disallowed. When unprivileged user namespaces or "rootless" containers are deployed on a system, the value should be set to a large non-zero value. The default value depends on the amount of memory in the system, approximately the total memory in kilobytes divided by 256.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 disables the use of user namespaces with the following commands.

Note: If unprivileged user namespaces or "rootless" containers are in use, this requirement is not applicable.

```
 $ sudo sysctl user.max_user_namespaces

 user.max_user_namespaces = 0
```

If the returned line does not have a value of "0" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
 $ sudo grep -r user.max_user_namespaces /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

 /etc/sysctl.d/99-sysctl.conf: user.max_user_namespaces = 0
```

If "user.max_user_namespaces" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system to disable the use of user namespaces by adding the following line to a file in the "/etc/sysctl.d" directory:

```
 user.max_user_namespaces = 0
```

Remove any configurations that conflict with the above from the following locations:

```
 /run/sysctl.d/*.conf
 /usr/local/lib/sysctl.d/*.conf
 /usr/lib/sysctl.d/*.conf
 /lib/sysctl.d/*.conf
 /etc/sysctl.conf
 /etc/sysctl.d/*.conf
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
 $ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.357 OL08-00-040285 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must use reverse path filtering on all IPv4 interfaces.

```
GROUP ID: V-248893
RULE ID: SV-248893r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Enabling reverse path filtering drops packets with source addresses that are not routable. There is no equivalent filter for IPv6 traffic. The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 uses reverse path filtering on all IPv4 interfaces with the following commands:

```
$ sudo sysctl net.ipv4.conf.all.rp_filter

net.ipv4.conf.all.rp_filter = 1
```

If the returned line does not have a value of "1" or "2" or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.ipv4.conf.all.rp_filter /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.all.rp_filter = 1
```

If "net.ipv4.conf.all.rp_filter" is not set to "1" or "2", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system to use reverse path filtering on all IPv4 interfaces by adding the following line to a file in the "/etc/sysctl.d" directory:

```
net.ipv4.conf.all.rp_filter = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.358 OL08-00-040286 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must enable hardening for the Berkeley Packet Filter Just-in-time compiler.

```
GROUP ID: V-248894
RULE ID: SV-248894r991589
```

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Enabling hardening for the Berkeley Packet Filter (BPF) Just-in-time (JIT) compiler aids in mitigating JIT spraying attacks. Setting the value to "2" enables JIT hardening for all users.

The sysctl --system command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored. /etc/sysctl.d/*.conf /run/sysctl.d/*.conf /usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf /etc/sysctl.conf

Internal Only - General

Audit:

Verify OL 8 enables hardening for the BPF JIT with the following commands:

```
$ sudo sysctl net.core.bpf_jit_harden

net.core.bpf_jit_harden = 2
```

If the returned line does not have a value of "2", or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
$ sudo grep -r net.core.bpf_jit_harden /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf

/etc/sysctl.d/99-sysctl.conf: net.core.bpf_jit_harden = 2
```

If "net.core.bpf_jit_harden" is not set to "2", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure OL 8 to enable hardening for the BPF JIT compiler by adding the following line to a file in the "/etc/sysctl.d" directory:

```
net.core.bpf_jit_harden = 2
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.359 OL08-00-040290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must be configured to prevent unrestricted mail relaying.

```
GROUP ID: V-248895
RULE ID: SV-248895r991589
```

Rationale:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay to send spam or for other unauthorized activity.

Audit:

Verify the system is configured to prevent unrestricted mail relaying.

Determine if "postfix" is installed with the following commands:

```
$ sudo yum list installed postfix

postfix.x86_64 2:3.3.1-9.el8
```

If postfix is not installed, this is not applicable.

If postfix is installed, determine if it is configured to reject connections from unknown or untrusted networks with the following command:

```
$ sudo postconf -n smtpd_client_restrictions

smtpd_client_restrictions = permit_mynetworks, reject
```

If the "smtpd_client_restrictions" parameter contains any entries other than "permit_mynetworks" and "reject", this is a finding.

Remediation:

If "postfix" is installed, modify the "/etc/postfix/main.cf" file to restrict client connections to the local network with the following command:

```
$ sudo postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.360 OL08-00-040300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The OL 8 file integrity tool must be configured to verify extended attributes.

```
GROUP ID: V-248896
RULE ID: SV-248896r991589
```

Rationale:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

OL 8 installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE).

Audit:

Verify the file integrity tool is configured to verify extended attributes.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Note: AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

```
$ sudo find / -name aide.conf
```

Check the "aide.conf" file to determine if the "xattrs" rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the "xattrs" rule follows:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

If the "xattrs" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or extended attributes are not being checked by another file integrity tool, this is a finding.

Remediation:

Configure the file integrity tool to check file and directory extended attributes.

If AIDE is installed, ensure the "xattrs" rule is present on all uncommented file and directory selection lists.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.361 OL08-00-040310 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The OL 8 file integrity tool must be configured to verify Access Control Lists (ACLs).

```
GROUP ID: V-248897
RULE ID: SV-248897r991589
```

Rationale:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

OL 8 installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE).

Audit:

Verify the file integrity tool is configured to verify ACLs.

Use the following command to determine if the file is in a location other than "/etc/aide/aide.conf":

```
$ sudo find / -name aide.conf
```

Check the "aide.conf" file to determine if the "acl" rule has been added to the rule list being applied to the files and directories selection lists with the following command:

```
$ sudo grep -E "[+]?acl" /etc/aide.conf

VarFile = OwnerMode+n+l+X+acl
```

If the "acl" rule is not being used on all selection lines in the "/etc/aide.conf" file or is commented out, or ACLs are not being checked by another file integrity tool, this is a finding.

Remediation:

Configure the file integrity tool to check file and directory ACLs.

If AIDE is installed, ensure the "acl" rule is present on all file and directory selection lists.

Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.362 OL08-00-040320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The graphical display manager must not be installed on OL 8 unless approved.

```
GROUP ID: V-248898
RULE ID: SV-248898r991589
```

Rationale:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. X Windows has a long history of security vulnerabilities and will not be used unless approved and documented.

Audit:

Verify that if the system has a display server installed, it is authorized.

Check for the display server package with the following example command:

```
$ sudo rpm -qa | grep xorg | grep server
```

Ask the System Administrator if use of the display server is an operational requirement.

If the use of a display server on the system is not documented with the Information System Security Officer (ISSO), this is a finding.

Remediation:

Document the requirement for a display server with the ISSO or remove the related packages with the following example command:

```
$ sudo rpm -e xorg-x11-server-common
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.363 OL08-00-040321 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The graphical display manager must not be the default target on OL 8 unless approved.

```
GROUP ID: V-252663
RULE ID: SV-252663r991589
```

Rationale:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. Graphical display managers have a long history of security vulnerabilities and must not be used, unless approved and documented.

Audit:

Verify that the system is configured to boot to the command line:

```
$ systemctl get-default

multi-user.target
```

If the system default target is not set to "multi-user.target" and the Information System Security Officer (ISSO) lacks a documented requirement for a graphical user interface, this is a finding.

Remediation:

Document the requirement for a graphical user interface with the ISSO or reinstall the operating system without the graphical user interface. If reinstallation is not feasible, then continue with the following procedure:

Open an SSH session and enter the following commands:

```
$ sudo systemctl set-default multi-user.target
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.364 OL08-00-040330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 network interfaces must not be in promiscuous mode.

```
GROUP ID: V-248899
RULE ID: SV-248899r991589
```

Rationale:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Audit:

Verify network interfaces are not in promiscuous mode unless approved by the ISSO and documented.

Check for the status with the following command:

```
$ sudo ip link | grep -i promisc
```

If network interfaces are found on the system in promiscuous mode and their use has not been approved by the ISSO and documented, this is a finding.

Remediation:

Configure network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.

Set the promiscuous mode of an interface to "off" with the following command:

```
$ sudo ip link set dev <devicename> multicast off promisc off
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.365 OL08-00-040340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 remote X connections for interactive users must be disabled unless to fulfill documented and validated mission requirements.

```
GROUP ID: V-248900
RULE ID: SV-248900r991589
```

Rationale:

The security risk of using X11 forwarding is that the client's X11 display server may be exposed to attack when the SSH client requests forwarding. A System Administrator may have a stance in which they want to protect clients that may expose themselves to attack by unwittingly requesting X11 forwarding, which can warrant a "no" setting.

X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X11 authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring if the "ForwardX11Trusted" option is also enabled.

If X11 services are not required for the system's intended function, they should be disabled or restricted as appropriate to the system’s needs.

Audit:

Verify "X11Forwarding" is disabled with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*x11forwarding'

X11Forwarding no
```

If the "X11Forwarding" keyword is set to "yes" and is not documented with the information system security officer (ISSO) as an operational requirement or is missing, this is a finding.

If conflicting results are returned, this is a finding.

Internal Only - General

Remediation:

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11Forwarding" keyword and set its value to "no" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
X11Forwarding no
```

The SSH service must be restarted for changes to take effect:

```
$ sudo systemctl restart sshd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.366 OL08-00-040341 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The OL 8 SSH daemon must prevent remote hosts from connecting to the proxy display.

```
GROUP ID: V-248901
RULE ID: SV-248901r991589
```

Rationale:

When X11 forwarding is enabled, there may be additional exposure to the server and client displays if the sshd proxy display is configured to listen on the wildcard address. By default, sshd binds the forwarding server to the loopback address and sets the hostname part of the DISPLAY environment variable to localhost. This prevents remote hosts from connecting to the proxy display.

Audit:

Verify the OL 8 SSH daemon prevents remote hosts from connecting to the proxy display.

Check the SSH "X11UseLocalhost" setting with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*x11uselocalhost'

X11UseLocalhost yes
```

If the "X11UseLocalhost" keyword is set to "no", is missing, or is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the OL 8 SSH daemon to prevent remote hosts from connecting to the proxy display.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11UseLocalhost" keyword and set its value to "yes" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
X11UseLocalhost yes
```


Internal Only - General

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.367 OL08-00-040342 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 SSH server must be configured to use only FIPS-validated key exchange algorithms.

```
GROUP ID: V-255898
RULE ID: SV-255898r991554
```

Rationale:

Without cryptographic integrity protections provided by FIPS-validated cryptographic algorithms, information can be viewed and altered by unauthorized users without detection.

OL 8 incorporates system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/opensshserver.config file.

The system will attempt to use the first algorithm presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest algorithm available to secure the SSH connection.

Audit:

Verify that the SSH server is configured to use only FIPS-validated key exchange algorithms:

```
 $ sudo grep -i kexalgorithms /etc/crypto-policies/back-
ends/opensshserver.config

 CRYPTO_POLICY='-oKexAlgorithms=ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-
sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-
sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512'
```

If the entries following "KexAlgorithms" have any algorithms defined other than "ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512", appear in a different order than shown, or are missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure the SSH server to use only FIPS-validated key exchange algorithms by adding or modifying the following line in "/etc/crypto-policies/back-ends/opensshserver.config":

```
-oKexAlgorithms=ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-
sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

Internal Only - General

1.368 OL08-00-040350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If the Trivial File Transfer Protocol (TFTP) server is required, the OL 8 TFTP daemon must be configured to operate in secure mode.

```
GROUP ID: V-248902
RULE ID: SV-248902r991589
```

Rationale:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Audit:

Verify the TFTP daemon is configured to operate in secure mode with the following commands:

```
$ sudo yum list installed tftp-server

tftp-server.x86_64 x.x-x.el8
```

If a TFTP server is not installed, this is not applicable.

If a TFTP server is installed, check for the server arguments with the following command:

```
$ sudo grep server_args /etc/xinetd.d/tftp

server_args = -s /var/lib/tftpboot
```

If the "server_args" line does not have a "-s" option and a subdirectory is not assigned, this is a finding.

Remediation:

Configure the TFTP daemon to operate in secure mode by adding the following line to "/etc/xinetd.d/tftp" (or modify the line to have the required value):

```
server_args = -s /var/lib/tftpboot
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.369 OL08-00-040360 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

A File Transfer Protocol (FTP) server package must not be installed unless mission essential on OL 8.

```
GROUP ID: V-248903
RULE ID: SV-248903r991589
```

Rationale:

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Audit:

Verify an FTP server has not been installed on the system with the following commands:

```
$ sudo yum list installed | grep ftpd

vsftpd-3.0.3.el8.x86_64.rpm
```

If an FTP server is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the FTP server package with the ISSO as an operational requirement or remove it from the system with the following command:

```
$ sudo yum remove vsftpd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.370 OL08-00-040370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the "gssproxy" package installed if not required for operational support.

```
GROUP ID: V-248904
RULE ID: SV-248904r1069143
```

Rationale:

Verify the operating system is configured to disable nonessential capabilities. The most secure way of ensuring a nonessential capability is disabled is to not have the capability installed.

When an application uses Generic Security Services API (GSSAPI), typically it will have direct access to its security credentials, and all cryptographic operations are performed in the application's process. This is undesirable, but "gssproxy" can help in almost all use cases. It provides privilege separation to applications using the GSSAPI: The gssproxy daemon runs on the system, holds the application's credentials, and performs operations on behalf of the application.

Audit:

Note: For Oracle Linux systems, if there is an operational need for gssproxy to be installed, this requirement is Not Applicable.

Determine if the "gssproxy" package is installed with the following command:

```
$ sudo yum list installed gssproxy
```

If the "gssproxy" package is installed, this is a finding.

Remediation:

Configure OL 8 to disable nonessential capabilities by removing the "gssproxy" package from the system with the following command:

```
$ sudo yum remove gssproxy
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.371 OL08-00-040380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the "iprutils" package installed if not required for operational support.

```
GROUP ID: V-248905
RULE ID: SV-248905r991589
```

Rationale:

The "iprutils" package provides a suite of utilities to manage and configure IBM Power Linux RAID Adapters supported by the IPR SCSI storage device driver. Disabling the "iprutils" package protects the system against exploitation of any flaws in its implementation.

Audit:

Determine if the "iprutils" package is installed with the following command:

```
$ sudo yum list installed iprutils
```

If the "iprutils" package is installed, this is a finding.

Remediation:

Configure OL 8 to disable non-essential capabilities by removing the "iprutils" package from the system with the following command:

```
$ sudo yum remove iprutils
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.372 OL08-00-040390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must not have the "tuned" package installed if not required for operational support.

```
GROUP ID: V-248906
RULE ID: SV-248906r991589
```

Rationale:

"Tuned" is a daemon that uses "udev" to monitor connected devices and statically and dynamically tunes system settings according to a selected profile. Disabling the "tuned" package protects the system against exploitation of any flaws in its implementation.

Audit:

Determine if the "tuned" package is installed with the following command:

```
$ sudo yum list installed tuned
```

If the "tuned" package is installed, this is a finding.

Remediation:

Configure OL 8 to disable non-essential capabilities by removing the "tuned" package from the system with the following command:

```
$ sudo yum remove tuned
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Internal Only - General

1.373 OL08-00-040400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 8 must prevent nonprivileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

```
GROUP ID: V-248907
RULE ID: SV-248907r958726
```

Rationale:

Preventing nonprivileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Nonprivileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from nonprivileged users.

Audit:

Verify the operating system prevents nonprivileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

Obtain a list of authorized users (other than system administrator and guest accounts) for the system.

Check the list against the system by using the following command:

```
$ sudo semanage login -l | more

Login Name    SELinux User    MLS/MCS Range    Service

__default__   user_u                s0-s0:c0.c1023        *
root                  unconfined_u  s0-s0:c0.c1023        *
system_u        system_u           s0-s0:c0.c1023        *
joe                    staff_u               s0-s0:c0.c1023        *
```

All administrators must be mapped to the "sysadm_u", "staff_u", or an appropriately tailored confined role as defined by the organization.

All authorized nonadministrative users must be mapped to the "user_u" role.

If they are not mapped in this way, this is a finding.

Internal Only - General

Remediation:

Configure OL 8 to prevent nonprivileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

Use the following command to map a new user to the "sysadm_u" role:

```
$ sudo semanage login -a -s sysadm_u <username>
```

Use the following command to map an existing user to the "sysadm_u" role:

```
$ sudo semanage login -m -s sysadm_u <username>
```

Use the following command to map a new user to the "staff_u" role:

```
$ sudo semanage login -a -s staff_u <username>
```

Use the following command to map an existing user to the "staff_u" role:

```
$ sudo semanage login -m -s staff_u <username>
```

Use the following command to map a new user to the "user_u" role:

```
$ sudo  semanage login -a -s user_u <username>
```

Use the following command to map an existing user to the "user_u" role:

```
$ sudo semanage login -m -s user_u <username>
```

Note: SELinux confined users mapped to sysadm_u are not allowed to log in to the system over SSH, by default. If this is a required function, it can be configured by setting the ssh_sysadm_login SELinux boolean to "on" with the following command:

```
$ sudo setsebool -P ssh_sysadm_login on
```

This must be documented with the information system security officer (ISSO) as an operational requirement.

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

Internal Only - General

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	OL08-00-010000 (Manual)	☐	☐
1.2	OL08-00-010010 (Manual)	☐	☐
1.3	OL08-00-010019 (Manual)	☐	☐
1.4	OL08-00-010020 (Manual)	☐	☐
1.5	OL08-00-010030 (Manual)	☐	☐
1.6	OL08-00-010040 (Manual)	☐	☐
1.7	OL08-00-010050 (Manual)	☐	☐
1.8	OL08-00-010049 (Manual)	☐	☐
1.9	OL08-00-010060 (Manual)	☐	☐
1.10	OL08-00-010070 (Manual)	☐	☐
1.11	OL08-00-010090 (Manual)	☐	☐
1.12	OL08-00-010100 (Manual)	☐	☐
1.13	OL08-00-010110 (Manual)	☐	☐
1.14	OL08-00-010120 (Manual)	☐	☐
1.15	OL08-00-010121 (Manual)	☐	☐
1.16	OL08-00-010130 (Manual)	☐	☐
1.17	OL08-00-010140 (Manual)	☐	☐
1.18	OL08-00-010141 (Manual)	☐	☐
1.19	OL08-00-010149 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	OL08-00-010150 (Manual)	☐	☐
1.21	OL08-00-010151 (Manual)	☐	☐
1.22	OL08-00-010152 (Manual)	☐	☐
1.23	OL08-00-010159 (Manual)	☐	☐
1.24	OL08-00-010160 (Manual)	☐	☐
1.25	OL08-00-010161 (Manual)	☐	☐
1.26	OL08-00-010162 (Manual)	☐	☐
1.27	OL08-00-010163 (Manual)	☐	☐
1.28	OL08-00-010170 (Manual)	☐	☐
1.29	OL08-00-010171 (Manual)	☐	☐
1.30	OL08-00-010190 (Manual)	☐	☐
1.31	OL08-00-010200 (Manual)	☐	☐
1.32	OL08-00-010201 (Manual)	☐	☐
1.33	OL08-00-010210 (Manual)	☐	☐
1.34	OL08-00-010220 (Manual)	☐	☐
1.35	OL08-00-010230 (Manual)	☐	☐
1.36	OL08-00-010240 (Manual)	☐	☐
1.37	OL08-00-010250 (Manual)	☐	☐
1.38	OL08-00-010260 (Manual)	☐	☐
1.39	OL08-00-010287 (Manual)	☐	☐
1.40	OL08-00-010290 (Manual)	☐	☐
1.41	OL08-00-010291 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	OL08-00-010292 (Manual)	☐	☐
1.43	OL08-00-010293 (Manual)	☐	☐
1.44	OL08-00-010294 (Manual)	☐	☐
1.45	OL08-00-010295 (Manual)	☐	☐
1.46	OL08-00-010300 (Manual)	☐	☐
1.47	OL08-00-010310 (Manual)	☐	☐
1.48	OL08-00-010320 (Manual)	☐	☐
1.49	OL08-00-010330 (Manual)	☐	☐
1.50	OL08-00-010331 (Manual)	☐	☐
1.51	OL08-00-010340 (Manual)	☐	☐
1.52	OL08-00-010341 (Manual)	☐	☐
1.53	OL08-00-010350 (Manual)	☐	☐
1.54	OL08-00-010351 (Manual)	☐	☐
1.55	OL08-00-010358 (Manual)	☐	☐
1.56	OL08-00-010359 (Manual)	☐	☐
1.57	OL08-00-010360 (Manual)	☐	☐
1.58	OL08-00-010370 (Manual)	☐	☐
1.59	OL08-00-010371 (Manual)	☐	☐
1.60	OL08-00-010372 (Manual)	☐	☐
1.61	OL08-00-010373 (Manual)	☐	☐
1.62	OL08-00-010375 (Manual)	☐	☐
1.63	OL08-00-010376 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	OL08-00-010374 (Manual)	☐	☐
1.65	OL08-00-010379 (Manual)	☐	☐
1.66	OL08-00-010380 (Manual)	☐	☐
1.67	OL08-00-010381 (Manual)	☐	☐
1.68	OL08-00-010382 (Manual)	☐	☐
1.69	OL08-00-010383 (Manual)	☐	☐
1.70	OL08-00-010384 (Manual)	☐	☐
1.71	OL08-00-010385 (Manual)	☐	☐
1.72	OL08-00-010390 (Manual)	☐	☐
1.73	OL08-00-010400 (Manual)	☐	☐
1.74	OL08-00-010410 (Manual)	☐	☐
1.75	OL08-00-010420 (Manual)	☐	☐
1.76	OL08-00-010421 (Manual)	☐	☐
1.77	OL08-00-010422 (Manual)	☐	☐
1.78	OL08-00-010423 (Manual)	☐	☐
1.79	OL08-00-010424 (Manual)	☐	☐
1.80	OL08-00-010430 (Manual)	☐	☐
1.81	OL08-00-010440 (Manual)	☐	☐
1.82	OL08-00-010450 (Manual)	☐	☐
1.83	OL08-00-010460 (Manual)	☐	☐
1.84	OL08-00-010470 (Manual)	☐	☐
1.85	OL08-00-010472 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	OL08-00-010473 (Manual)	☐	☐
1.87	OL08-00-010480 (Manual)	☐	☐
1.88	OL08-00-010490 (Manual)	☐	☐
1.89	OL08-00-010500 (Manual)	☐	☐
1.90	OL08-00-010520 (Manual)	☐	☐
1.91	OL08-00-010521 (Manual)	☐	☐
1.92	OL08-00-010522 (Manual)	☐	☐
1.93	OL08-00-010540 (Manual)	☐	☐
1.94	OL08-00-010541 (Manual)	☐	☐
1.95	OL08-00-010542 (Manual)	☐	☐
1.96	OL08-00-010543 (Manual)	☐	☐
1.97	OL08-00-010544 (Manual)	☐	☐
1.98	OL08-00-010550 (Manual)	☐	☐
1.99	OL08-00-010561 (Manual)	☐	☐
1.100	OL08-00-010570 (Manual)	☐	☐
1.101	OL08-00-010571 (Manual)	☐	☐
1.102	OL08-00-010572 (Manual)	☐	☐
1.103	OL08-00-010580 (Manual)	☐	☐
1.104	OL08-00-010590 (Manual)	☐	☐
1.105	OL08-00-010600 (Manual)	☐	☐
1.106	OL08-00-010610 (Manual)	☐	☐
1.107	OL08-00-010620 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	OL08-00-010630 (Manual)	☐	☐
1.109	OL08-00-010640 (Manual)	☐	☐
1.110	OL08-00-010650 (Manual)	☐	☐
1.111	OL08-00-010660 (Manual)	☐	☐
1.112	OL08-00-010670 (Manual)	☐	☐
1.113	OL08-00-010671 (Manual)	☐	☐
1.114	OL08-00-010672 (Manual)	☐	☐
1.115	OL08-00-010673 (Manual)	☐	☐
1.116	OL08-00-010674 (Manual)	☐	☐
1.117	OL08-00-010675 (Manual)	☐	☐
1.118	OL08-00-010680 (Manual)	☐	☐
1.119	OL08-00-010690 (Manual)	☐	☐
1.120	OL08-00-010700 (Manual)	☐	☐
1.121	OL08-00-010710 (Manual)	☐	☐
1.122	OL08-00-010720 (Manual)	☐	☐
1.123	OL08-00-010730 (Manual)	☐	☐
1.124	OL08-00-010731 (Manual)	☐	☐
1.125	OL08-00-010740 (Manual)	☐	☐
1.126	OL08-00-010760 (Manual)	☐	☐
1.127	OL08-00-010750 (Manual)	☐	☐
1.128	OL08-00-010741 (Manual)	☐	☐
1.129	OL08-00-010780 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	OL08-00-010790 (Manual)	☐	☐
1.131	OL08-00-010770 (Manual)	☐	☐
1.132	OL08-00-010820 (Manual)	☐	☐
1.133	OL08-00-010800 (Manual)	☐	☐
1.134	OL08-00-010830 (Manual)	☐	☐
1.135	OL08-00-020000 (Manual)	☐	☐
1.136	OL08-00-020010 (Manual)	☐	☐
1.137	OL08-00-020011 (Manual)	☐	☐
1.138	OL08-00-020012 (Manual)	☐	☐
1.139	OL08-00-020013 (Manual)	☐	☐
1.140	OL08-00-020014 (Manual)	☐	☐
1.141	OL08-00-020015 (Manual)	☐	☐
1.142	OL08-00-020016 (Manual)	☐	☐
1.143	OL08-00-020017 (Manual)	☐	☐
1.144	OL08-00-020018 (Manual)	☐	☐
1.145	OL08-00-020019 (Manual)	☐	☐
1.146	OL08-00-020020 (Manual)	☐	☐
1.147	OL08-00-020021 (Manual)	☐	☐
1.148	OL08-00-020022 (Manual)	☐	☐
1.149	OL08-00-020023 (Manual)	☐	☐
1.150	OL08-00-020024 (Manual)	☐	☐
1.151	OL08-00-020025 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	OL08-00-020026 (Manual)	☐	☐
1.153	OL08-00-020027 (Manual)	☐	☐
1.154	OL08-00-020028 (Manual)	☐	☐
1.155	OL08-00-020030 (Manual)	☐	☐
1.156	OL08-00-020031 (Manual)	☐	☐
1.157	OL08-00-020032 (Manual)	☐	☐
1.158	OL08-00-020035 (Manual)	☐	☐
1.159	OL08-00-020043 (Manual)	☐	☐
1.160	OL08-00-020050 (Manual)	☐	☐
1.161	OL08-00-020060 (Manual)	☐	☐
1.162	OL08-00-020080 (Manual)	☐	☐
1.163	OL08-00-020081 (Manual)	☐	☐
1.164	OL08-00-020082 (Manual)	☐	☐
1.165	OL08-00-020090 (Manual)	☐	☐
1.166	OL08-00-020100 (Manual)	☐	☐
1.167	OL08-00-020101 (Manual)	☐	☐
1.168	OL08-00-020102 (Manual)	☐	☐
1.169	OL08-00-020103 (Manual)	☐	☐
1.170	OL08-00-020104 (Manual)	☐	☐
1.171	OL08-00-020110 (Manual)	☐	☐
1.172	OL08-00-020120 (Manual)	☐	☐
1.173	OL08-00-020130 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	OL08-00-020140 (Manual)	☐	☐
1.175	OL08-00-020150 (Manual)	☐	☐
1.176	OL08-00-020160 (Manual)	☐	☐
1.177	OL08-00-020170 (Manual)	☐	☐
1.178	OL08-00-020180 (Manual)	☐	☐
1.179	OL08-00-020190 (Manual)	☐	☐
1.180	OL08-00-020200 (Manual)	☐	☐
1.181	OL08-00-020210 (Manual)	☐	☐
1.182	OL08-00-020230 (Manual)	☐	☐
1.183	OL08-00-020231 (Manual)	☐	☐
1.184	OL08-00-020240 (Manual)	☐	☐
1.185	OL08-00-020250 (Manual)	☐	☐
1.186	OL08-00-020260 (Manual)	☐	☐
1.187	OL08-00-020261 (Manual)	☐	☐
1.188	OL08-00-020262 (Manual)	☐	☐
1.189	OL08-00-020263 (Manual)	☐	☐
1.190	OL08-00-020264 (Manual)	☐	☐
1.191	OL08-00-020270 (Manual)	☐	☐
1.192	OL08-00-020280 (Manual)	☐	☐
1.193	OL08-00-020290 (Manual)	☐	☐
1.194	OL08-00-020300 (Manual)	☐	☐
1.195	OL08-00-020310 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.196	OL08-00-020320 (Manual)	☐	☐
1.197	OL08-00-020330 (Manual)	☐	☐
1.198	OL08-00-020331 (Manual)	☐	☐
1.199	OL08-00-020332 (Manual)	☐	☐
1.200	OL08-00-020340 (Manual)	☐	☐
1.201	OL08-00-020350 (Manual)	☐	☐
1.202	OL08-00-020351 (Manual)	☐	☐
1.203	OL08-00-020352 (Manual)	☐	☐
1.204	OL08-00-020353 (Manual)	☐	☐
1.205	OL08-00-030000 (Manual)	☐	☐
1.206	OL08-00-030010 (Manual)	☐	☐
1.207	OL08-00-030020 (Manual)	☐	☐
1.208	OL08-00-030030 (Manual)	☐	☐
1.209	OL08-00-030040 (Manual)	☐	☐
1.210	OL08-00-030060 (Manual)	☐	☐
1.211	OL08-00-030061 (Manual)	☐	☐
1.212	OL08-00-030062 (Manual)	☐	☐
1.213	OL08-00-030063 (Manual)	☐	☐
1.214	OL08-00-030070 (Manual)	☐	☐
1.215	OL08-00-030080 (Manual)	☐	☐
1.216	OL08-00-030090 (Manual)	☐	☐
1.217	OL08-00-030100 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.218	OL08-00-030110 (Manual)	☐	☐
1.219	OL08-00-030120 (Manual)	☐	☐
1.220	OL08-00-030121 (Manual)	☐	☐
1.221	OL08-00-030122 (Manual)	☐	☐
1.222	OL08-00-030130 (Manual)	☐	☐
1.223	OL08-00-030140 (Manual)	☐	☐
1.224	OL08-00-030150 (Manual)	☐	☐
1.225	OL08-00-030160 (Manual)	☐	☐
1.226	OL08-00-030170 (Manual)	☐	☐
1.227	OL08-00-030171 (Manual)	☐	☐
1.228	OL08-00-030172 (Manual)	☐	☐
1.229	OL08-00-030180 (Manual)	☐	☐
1.230	OL08-00-030181 (Manual)	☐	☐
1.231	OL08-00-030190 (Manual)	☐	☐
1.232	OL08-00-030200 (Manual)	☐	☐
1.233	OL08-00-030250 (Manual)	☐	☐
1.234	OL08-00-030260 (Manual)	☐	☐
1.235	OL08-00-030280 (Manual)	☐	☐
1.236	OL08-00-030290 (Manual)	☐	☐
1.237	OL08-00-030300 (Manual)	☐	☐
1.238	OL08-00-030301 (Manual)	☐	☐
1.239	OL08-00-030302 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.240	OL08-00-030310 (Manual)	☐	☐
1.241	OL08-00-030311 (Manual)	☐	☐
1.242	OL08-00-030312 (Manual)	☐	☐
1.243	OL08-00-030313 (Manual)	☐	☐
1.244	OL08-00-030314 (Manual)	☐	☐
1.245	OL08-00-030315 (Manual)	☐	☐
1.246	OL08-00-030316 (Manual)	☐	☐
1.247	OL08-00-030317 (Manual)	☐	☐
1.248	OL08-00-030320 (Manual)	☐	☐
1.249	OL08-00-030330 (Manual)	☐	☐
1.250	OL08-00-030340 (Manual)	☐	☐
1.251	OL08-00-030350 (Manual)	☐	☐
1.252	OL08-00-030360 (Manual)	☐	☐
1.253	OL08-00-030361 (Manual)	☐	☐
1.254	OL08-00-030370 (Manual)	☐	☐
1.255	OL08-00-030390 (Manual)	☐	☐
1.256	OL08-00-030400 (Manual)	☐	☐
1.257	OL08-00-030410 (Manual)	☐	☐
1.258	OL08-00-030420 (Manual)	☐	☐
1.259	OL08-00-030480 (Manual)	☐	☐
1.260	OL08-00-030490 (Manual)	☐	☐
1.261	OL08-00-030550 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.262	OL08-00-030560 (Manual)	☐	☐
1.263	OL08-00-030570 (Manual)	☐	☐
1.264	OL08-00-030580 (Manual)	☐	☐
1.265	OL08-00-030590 (Manual)	☐	☐
1.266	OL08-00-030600 (Manual)	☐	☐
1.267	OL08-00-030601 (Manual)	☐	☐
1.268	OL08-00-030602 (Manual)	☐	☐
1.269	OL08-00-030603 (Manual)	☐	☐
1.270	OL08-00-030610 (Manual)	☐	☐
1.271	OL08-00-030620 (Manual)	☐	☐
1.272	OL08-00-030630 (Manual)	☐	☐
1.273	OL08-00-030640 (Manual)	☐	☐
1.274	OL08-00-030650 (Manual)	☐	☐
1.275	OL08-00-030660 (Manual)	☐	☐
1.276	OL08-00-030670 (Manual)	☐	☐
1.277	OL08-00-030680 (Manual)	☐	☐
1.278	OL08-00-030690 (Manual)	☐	☐
1.279	OL08-00-030700 (Manual)	☐	☐
1.280	OL08-00-030710 (Manual)	☐	☐
1.281	OL08-00-030720 (Manual)	☐	☐
1.282	OL08-00-030730 (Manual)	☐	☐
1.283	OL08-00-030731 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.284	OL08-00-030740 (Manual)	☐	☐
1.285	OL08-00-030741 (Manual)	☐	☐
1.286	OL08-00-030742 (Manual)	☐	☐
1.287	OL08-00-040000 (Manual)	☐	☐
1.288	OL08-00-040001 (Manual)	☐	☐
1.289	OL08-00-040002 (Manual)	☐	☐
1.290	OL08-00-040004 (Manual)	☐	☐
1.291	OL08-00-040010 (Manual)	☐	☐
1.292	OL08-00-040020 (Manual)	☐	☐
1.293	OL08-00-040021 (Manual)	☐	☐
1.294	OL08-00-040022 (Manual)	☐	☐
1.295	OL08-00-040023 (Manual)	☐	☐
1.296	OL08-00-040024 (Manual)	☐	☐
1.297	OL08-00-040025 (Manual)	☐	☐
1.298	OL08-00-040026 (Manual)	☐	☐
1.299	OL08-00-040030 (Manual)	☐	☐
1.300	OL08-00-040070 (Manual)	☐	☐
1.301	OL08-00-040080 (Manual)	☐	☐
1.302	OL08-00-040090 (Manual)	☐	☐
1.303	OL08-00-040100 (Manual)	☐	☐
1.304	OL08-00-040101 (Manual)	☐	☐
1.305	OL08-00-040110 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.306	OL08-00-040111 (Manual)	☐	☐
1.307	OL08-00-040120 (Manual)	☐	☐
1.308	OL08-00-040121 (Manual)	☐	☐
1.309	OL08-00-040122 (Manual)	☐	☐
1.310	OL08-00-040123 (Manual)	☐	☐
1.311	OL08-00-040124 (Manual)	☐	☐
1.312	OL08-00-040125 (Manual)	☐	☐
1.313	OL08-00-040126 (Manual)	☐	☐
1.314	OL08-00-040127 (Manual)	☐	☐
1.315	OL08-00-040128 (Manual)	☐	☐
1.316	OL08-00-040129 (Manual)	☐	☐
1.317	OL08-00-040130 (Manual)	☐	☐
1.318	OL08-00-040131 (Manual)	☐	☐
1.319	OL08-00-040132 (Manual)	☐	☐
1.320	OL08-00-040133 (Manual)	☐	☐
1.321	OL08-00-040134 (Manual)	☐	☐
1.322	OL08-00-040135 (Manual)	☐	☐
1.323	OL08-00-040136 (Manual)	☐	☐
1.324	OL08-00-040137 (Manual)	☐	☐
1.325	OL08-00-040139 (Manual)	☐	☐
1.326	OL08-00-040140 (Manual)	☐	☐
1.327	OL08-00-040141 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.328	OL08-00-040150 (Manual)	☐	☐
1.329	OL08-00-040159 (Manual)	☐	☐
1.330	OL08-00-040160 (Manual)	☐	☐
1.331	OL08-00-040161 (Manual)	☐	☐
1.332	OL08-00-040170 (Manual)	☐	☐
1.333	OL08-00-040171 (Manual)	☐	☐
1.334	OL08-00-040172 (Manual)	☐	☐
1.335	OL08-00-040180 (Manual)	☐	☐
1.336	OL08-00-040190 (Manual)	☐	☐
1.337	OL08-00-040200 (Manual)	☐	☐
1.338	OL08-00-040209 (Manual)	☐	☐
1.339	OL08-00-040210 (Manual)	☐	☐
1.340	OL08-00-040220 (Manual)	☐	☐
1.341	OL08-00-040230 (Manual)	☐	☐
1.342	OL08-00-040239 (Manual)	☐	☐
1.343	OL08-00-040240 (Manual)	☐	☐
1.344	OL08-00-040249 (Manual)	☐	☐
1.345	OL08-00-040250 (Manual)	☐	☐
1.346	OL08-00-040259 (Manual)	☐	☐
1.347	OL08-00-040260 (Manual)	☐	☐
1.348	OL08-00-040261 (Manual)	☐	☐
1.349	OL08-00-040262 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.350	OL08-00-040270 (Manual)	☐	☐
1.351	OL08-00-040279 (Manual)	☐	☐
1.352	OL08-00-040280 (Manual)	☐	☐
1.353	OL08-00-040281 (Manual)	☐	☐
1.354	OL08-00-040282 (Manual)	☐	☐
1.355	OL08-00-040283 (Manual)	☐	☐
1.356	OL08-00-040284 (Manual)	☐	☐
1.357	OL08-00-040285 (Manual)	☐	☐
1.358	OL08-00-040286 (Manual)	☐	☐
1.359	OL08-00-040290 (Manual)	☐	☐
1.360	OL08-00-040300 (Manual)	☐	☐
1.361	OL08-00-040310 (Manual)	☐	☐
1.362	OL08-00-040320 (Manual)	☐	☐
1.363	OL08-00-040321 (Manual)	☐	☐
1.364	OL08-00-040330 (Manual)	☐	☐
1.365	OL08-00-040340 (Manual)	☐	☐
1.366	OL08-00-040341 (Manual)	☐	☐
1.367	OL08-00-040342 (Manual)	☐	☐
1.368	OL08-00-040350 (Manual)	☐	☐
1.369	OL08-00-040360 (Manual)	☐	☐
1.370	OL08-00-040370 (Manual)	☐	☐
1.371	OL08-00-040380 (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.372	OL08-00-040390 (Manual)	☐	☐
1.373	OL08-00-040400 (Manual)	☐	☐

Internal Only - General

Appendix: Change History

Date	Version	Changes for this version
Aug 26, 2025	1.0.0	Initial CIS Release

Internal Only - General