CIS Amazon Linux 2023 STIG Benchmark

v1.0.0 - 03-31-2026

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 *7*

Important Usage Information **7**

Key Stakeholders **7**

Apply the Correct Version of a Benchmark **8**

Exceptions **8**

Remediation **9**

Summary **9**

Target Technology Details **10**

Intended Audience **10**

Typographical Conventions **11**

Recommendation Definitions *12*

Title **12**

Assessment Status **12**

Automated **12**

Manual **12**

Profile **12**

Description **12**

Rationale Statement **12**

Audit Procedure **13**

Remediation Procedure **13**

Additional Information **13**

Profile Definitions **14**

Acknowledgements **15**

Recommendations *16*

1 STIG RULES **16**

1.1 AZLX-23-000100 (Manual) 17

1.2 AZLX-23-000110 (Manual) 19

1.3 AZLX-23-000115 (Automated) 21

1.4 AZLX-23-000120 (Automated) 23

1.5 AZLX-23-000125 (Automated) 25

1.6 AZLX-23-000130 (Manual) 27

1.7 AZLX-23-000135 (Automated) 29

1.8 AZLX-23-000200 (Automated) 30

1.9 AZLX-23-000205 (Automated) 32

1.10 AZLX-23-000210 (Automated) 34

1.11 AZLX-23-000215 (Automated) 36

1.12 AZLX-23-000220 (Automated) 38

Internal Only - General

1.13 AZLX-23-000225 (Automated) 40
1.14 AZLX-23-000300 (Automated) 42
1.15 AZLX-23-000305 (Automated) 44
1.16 AZLX-23-000310 (Automated) 46
1.17 AZLX-23-000315 (Automated) 48
1.18 AZLX-23-000320 (Automated) 50
1.19 AZLX-23-001000 (Automated) 52
1.20 AZLX-23-001005 (Automated) 53
1.21 AZLX-23-001010 (Automated) 54
1.22 AZLX-23-001015 (Automated) 55
1.23 AZLX-23-001020 (Automated) 56
1.24 AZLX-23-001025 (Automated) 57
1.25 AZLX-23-001030 (Automated) 62
1.26 AZLX-23-001035 (Automated) 67
1.27 AZLX-23-001040 (Automated) 68
1.28 AZLX-23-001045 (Automated) 70
1.29 AZLX-23-001050 (Automated) 72
1.30 AZLX-23-001055 (Automated) 73
1.31 AZLX-23-001060 (Automated) 74
1.32 AZLX-23-001065 (Automated) 76
1.33 AZLX-23-001070 (Automated) 79
1.34 AZLX-23-001075 (Automated) 82
1.35 AZLX-23-001080 (Automated) 84
1.36 AZLX-23-001085 (Manual) 86
1.37 AZLX-23-001090 (Automated) 88
1.38 AZLX-23-001095 (Automated) 90
1.39 AZLX-23-001105 (Automated) 91
1.40 AZLX-23-001110 (Automated) 93
1.41 AZLX-23-001115 (Automated) 95
1.42 AZLX-23-001120 (Automated) 96
1.43 AZLX-23-001125 (Automated) 98
1.44 AZLX-23-001130 (Automated) 100
1.45 AZLX-23-001180 (Automated) 102
1.46 AZLX-23-001185 (Automated) 104
1.47 AZLX-23-001195 (Automated) 106
1.48 AZLX-23-001200 (Automated) 108
1.49 AZLX-23-001205 (Automated) 110
1.50 AZLX-23-001210 (Automated) 112
1.51 AZLX-23-001215 (Automated) 114
1.52 AZLX-23-001220 (Automated) 116
1.53 AZLX-23-001225 (Automated) 118
1.54 AZLX-23-001230 (Automated) 120
1.55 AZLX-23-001235 (Automated) 122
1.56 AZLX-23-001240 (Automated) 124
1.57 AZLX-23-001245 (Automated) 126
1.58 AZLX-23-001250 (Automated) 128
1.59 AZLX-23-001255 (Automated) 130
1.60 AZLX-23-001260 (Automated) 132
1.61 AZLX-23-001265 (Automated) 134
1.62 AZLX-23-001270 (Automated) 136
1.63 AZLX-23-001275 (Automated) 140
1.64 AZLX-23-001280 (Automated) 142
1.65 AZLX-23-001285 (Automated) 144
1.66 AZLX-23-001290 (Automated) 147
1.67 AZLX-23-001295 (Manual) 149
1.68 AZLX-23-001300 (Automated) 151

Internal Only - General

1.69 AZLX-23-001305 (Automated)..... 153
1.70 AZLX-23-001310 (Manual)..... 155
1.71 AZLX-23-001315 (Manual)..... 158
1.72 AZLX-23-002000 (Manual)..... 160
1.73 AZLX-23-002005 (Automated)..... 163
1.74 AZLX-23-002015 (Manual)..... 166
1.75 AZLX-23-002020 (Automated)..... 168
1.76 AZLX-23-002025 (Automated)..... 169
1.77 AZLX-23-002030 (Automated)..... 170
1.78 AZLX-23-002035 (Automated)..... 172
1.79 AZLX-23-002040 (Automated)..... 173
1.80 AZLX-23-002045 (Automated)..... 175
1.81 AZLX-23-002050 (Automated)..... 176
1.82 AZLX-23-002055 (Automated)..... 178
1.83 AZLX-23-002060 (Automated)..... 180
1.84 AZLX-23-002065 (Automated)..... 181
1.85 AZLX-23-002070 (Automated)..... 182
1.86 AZLX-23-002075 (Automated)..... 183
1.87 AZLX-23-002080 (Manual)..... 185
1.88 AZLX-23-002085 (Automated)..... 187
1.89 AZLX-23-002090 (Automated)..... 190
1.90 AZLX-23-002095 (Automated)..... 193
1.91 AZLX-23-002100 (Automated)..... 196
1.92 AZLX-23-002105 (Automated)..... 199
1.93 AZLX-23-002110 (Automated)..... 202
1.94 AZLX-23-002115 (Automated)..... 204
1.95 AZLX-23-002120 (Automated)..... 207
1.96 AZLX-23-002125 (Automated)..... 210
1.97 AZLX-23-002130 (Automated)..... 213
1.98 AZLX-23-002135 (Automated)..... 216
1.99 AZLX-23-002140 (Automated)..... 219
1.100 AZLX-23-002145 (Automated)..... 222
1.101 AZLX-23-002150 (Automated)..... 225
1.102 AZLX-23-002155 (Automated)..... 228
1.103 AZLX-23-002160 (Automated)..... 231
1.104 AZLX-23-002165 (Automated)..... 233
1.105 AZLX-23-002175 (Automated)..... 236
1.106 AZLX-23-002180 (Automated)..... 237
1.107 AZLX-23-002185 (Automated)..... 238
1.108 AZLX-23-002190 (Automated)..... 239
1.109 AZLX-23-002195 (Automated)..... 241
1.110 AZLX-23-002200 (Automated)..... 243
1.111 AZLX-23-002205 (Automated)..... 245
1.112 AZLX-23-002210 (Automated)..... 249
1.113 AZLX-23-002215 (Automated)..... 252
1.114 AZLX-23-002220 (Automated)..... 254
1.115 AZLX-23-002225 (Automated)..... 256
1.116 AZLX-23-002230 (Automated)..... 258
1.117 AZLX-23-002235 (Automated)..... 260
1.118 AZLX-23-002240 (Automated)..... 262
1.119 AZLX-23-002245 (Automated)..... 264
1.120 AZLX-23-002250 (Automated)..... 267
1.121 AZLX-23-002255 (Automated)..... 270
1.122 AZLX-23-002260 (Automated)..... 273
1.123 AZLX-23-002265 (Automated)..... 274
1.124 AZLX-23-002270 (Automated)..... 276

Internal Only - General

1.125 AZLX-23-002275 (Automated)....278
1.126 AZLX-23-002280 (Automated)....280
1.127 AZLX-23-002285 (Automated)....282
1.128 AZLX-23-002290 (Automated)....284
1.129 AZLX-23-002295 (Automated)....286
1.130 AZLX-23-002300 (Automated)....287
1.131 AZLX-23-002305 (Automated)....289
1.132 AZLX-23-002315 (Automated)....291
1.133 AZLX-23-002320 (Automated)....293
1.134 AZLX-23-002325 (Automated)....294
1.135 AZLX-23-002330 (Automated)....295
1.136 AZLX-23-002335 (Automated)....297
1.137 AZLX-23-002340 (Automated)....298
1.138 AZLX-23-002345 (Automated)....299
1.139 AZLX-23-002350 (Automated)....301
1.140 AZLX-23-002355 (Automated)....303
1.141 AZLX-23-002360 (Automated)....305
1.142 AZLX-23-002365 (Automated)....307
1.143 AZLX-23-002370 (Automated)....309
1.144 AZLX-23-002375 (Automated)....311
1.145 AZLX-23-002380 (Automated)....313
1.146 AZLX-23-002385 (Automated)....315
1.147 AZLX-23-002390 (Automated)....317
1.148 AZLX-23-002395 (Automated)....319
1.149 AZLX-23-002396 (Automated)....321
1.150 AZLX-23-002400 (Automated)....323
1.151 AZLX-23-002405 (Automated)....324
1.152 AZLX-23-002410 (Automated)....325
1.153 AZLX-23-002415 (Manual)....327
1.154 AZLX-23-002420 (Automated)....329
1.155 AZLX-23-002425 (Automated)....331
1.156 AZLX-23-002430 (Automated)....332
1.157 AZLX-23-002435 (Manual)....334
1.158 AZLX-23-002440 (Automated)....336
1.159 AZLX-23-002445 (Automated)....337
1.160 AZLX-23-002450 (Automated)....338
1.161 AZLX-23-002455 (Automated)....340
1.162 AZLX-23-002460 (Automated)....341
1.163 AZLX-23-002465 (Automated)....342
1.164 AZLX-23-002470 (Automated)....344
1.165 AZLX-23-002475 (Manual)....345
1.166 AZLX-23-002480 (Automated)....347
1.167 AZLX-23-002485 (Automated)....349
1.168 AZLX-23-002489 (Automated)....351
1.169 AZLX-23-002490 (Automated)....353
1.170 AZLX-23-002495 (Automated)....355
1.171 AZLX-23-002500 (Automated)....357
1.172 AZLX-23-002505 (Automated)....359
1.173 AZLX-23-002510 (Automated)....361
1.174 AZLX-23-002515 (Automated)....363
1.175 AZLX-23-002520 (Automated)....366
1.176 AZLX-23-002535 (Automated)....368
1.177 AZLX-23-002540 (Automated)....370
1.178 AZLX-23-002555 (Automated)....372
1.179 AZLX-23-002560 (Manual)....373
1.180 AZLX-23-002565 (Manual)....375

Internal Only - General

1.181 AZLX-23-002570 (Automated)....377
1.182 AZLX-23-002575 (Automated)....379
1.183 AZLX-23-002580 (Automated)....381
1.184 AZLX-23-002590 (Automated)....382
1.185 AZLX-23-002585 (Automated)....383
1.186 AZLX-23-002595 (Automated)....384
1.187 AZLX-23-002600 (Automated)....385
1.188 AZLX-23-002605 (Manual)....386
1.189 AZLX-23-002610 (Automated)....388
1.190 AZLX-23-002615 (Automated)....389
1.191 AZLX-23-002620 (Automated)....390
1.192 AZLX-23-005000 (Automated)....391
Appendix: Summary Table....393
Appendix: Change History....402

Internal Only - General

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Internal Only - General

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Internal Only - General

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Internal Only - General

Target Technology Details

Amazon Linux 2023 Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 05 Jan 2026

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 Amazon Linux 2023 and are looking to comply with the STIG guidance

Internal Only - General

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

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 for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

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

Internal Only - General

Audit Procedure

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

Remediation Procedure

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

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

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 Amazon Linux 2023

Internal Only - General

Recommendations

1 STIG RULES

Amazon Linux 2023

Amazon Linux 2023 Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 05 Jan 2026

CLASSIFICATION unclassified

Internal Only - General

1.1 AZLX-23-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 local disk partitions must implement cryptographic mechanisms to prevent unauthorized disclosure or modification of all information that requires at rest protection.

```
GROUP ID: V-273994
RULE ID: SV-273994r1119970
```

Rationale:

Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive, when used for backups) within an operating system.

This requirement addresses protection of user-generated data, as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

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

Audit:

Verify Amazon Linux 2023 is configured so that all partitions are encrypted with the following command:

```
$ sudo blkid
```

/dev/xvda1: UUID="ed0acbe9-bd05-495e-a9ac-cb615b29327d" TYPE="crypto_LUKS"

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

If any partitions other than the boot partition, bios partition or pseudo file systems (such as /proc or /sys) are not type "crypto_LUKS", this is a finding.

Remediation:

Configure Amazon Linux 2023 to protect the confidentiality and integrity of all information at rest.

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.

Internal Only - General

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

1.2 AZLX-23-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure cryptographic verification of vendor software packages.

```
GROUP ID: V-273995
RULE ID: SV-273995r1119973
```

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. Amazon Linux cryptographically signs all software packages, which includes updates, with a GPG key to Verify they are valid.

Audit:

Verify Amazon Linux 2023 package-signing keys are installed on the system and verify their fingerprints match vendor values.

Note: For Amazon Linux 2023 software packages, AWS uses GPG keys defined in key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-amazon-linux-2023" by default.

List Amazon Linux GPG keys installed on the system:

```
$ sudo rpm -q gpg-pubkey --qf "%{NAME}-%{VERSION}-%{RELEASE} %{SUMMARY}\n"
```

gpg-pubkey-d832c631-6515c85e Amazon Linux amazon-linux@amazon.com public key

If there is no Amazon Linux GPG key installed, this is a finding.

Extract the fingerprint from the key with this command:

```
$ sudo gpg -q --keyid-format short --with-fingerprint /etc/pki/rpm-gpg/RPM-
GPG-KEY-amazon-linux-2023
```

pub rsa4096/D832C631 2022-12-08 [SC] Key fingerprint = B21C 50FA 44A9 9720 EAA7 2F7F E951 904A D832 C631 uid Amazon Linux amazon-linux@amazon.com

Compare the Key fingerprint with the key fingerprint from Amazon Documentation and instructions at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/verify-keys.html

If key fingerprints do not match, or the key file is missing, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to have the public key for verifying RPM packages to be installed with the "system-release" package.

Install the system-release installation with the following command:

```
$ sudo dnf install -y system-release
```

Ensure cryptographic verification of software packages is enabled by editing /etc/dnf/dnf.conf and under '[main]' in the configuration file add:

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

Internal Only - General

1.3 AZLX-23-000115 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must check the GPG signature of locally installed software packages before installation.

```
GROUP ID: V-273996
RULE ID: SV-273996r1119976
```

Rationale:

Changes to any software components can have significant effects on the overall security of Amazon Linux 2023. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify Amazon Linux 2023 is configured so that dnf always checks the GPG signature of locally installed software packages before installation:

```
$ grep localpkg_gpgcheck /etc/dnf/dnf.conf
```

localpkg_gpgcheck=1

If "localpkg_gpgcheck" is not set to "1" or "True", or if the option is missing or commented out, ask the system administrator how the GPG signatures of local software packages are being verified.

If there is no process to verify GPG signatures approved by the organization, this is a finding.

Remediation:

Configure Amazon Linux 2023 to always check the GPG signature of local software packages before installation.

Add or update the following line in the [main] section of the /etc/dnf/dnf.conf file:

localpkg_gpgcheck=1

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

Internal Only - General

1.4 AZLX-23-000120 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must check the GPG signature of software packages originating from external software repositories before installation.

```
GROUP ID: V-273997
RULE ID: SV-273997r1119979
```

Rationale:

Changes to any software components can have significant effects on the overall security of Amazon Linux 2023. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify Amazon Linux 2023 is configured so that dnf always checks the GPG signature of software packages originating from external software repositories before installation:

```
$ grep -w gpgcheck /etc/dnf/dnf.conf
```

gpgcheck=1

If "gpgcheck" is not set to "1" or "True", or if the option is missing or commented out, ask the system administrator how the GPG signatures of software packages are being verified.

If there is no process to verify GPG signatures approved by the organization, this is a finding.

Remediation:

Configure Amazon Linux 2023 to always check the GPG signature of software packages originating from external software repositories before installation.

Add or update the following line in the [main] section of the /etc/dnf/dnf.conf file:

gpgcheck=1

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

Internal Only - General

1.5 AZLX-23-000125 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must have GPG signature verification enabled for all software repositories.

```
GROUP ID: V-273998
RULE ID: SV-273998r1119982
```

Rationale:

Changes to any software components can have significant effects on the overall security of Amazon Linux 2023. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify Amazon Linux 2023 software repositories enforce a signature check on the packages prior to allowing installation with the following command:

```
$ grep -w gpgcheck /etc/yum.repos.d/*.repo | more
```

/etc/yum.repos.d/amazonlinux.repo:gpgcheck=1
/etc/yum.repos.d/amazonlinux.repo:gpgcheck=1
/etc/yum.repos.d/amazonlinux.repo:gpgcheck=1 /etc/yum.repos.d/kernel-livepatch.repo:gpgcheck=1 /etc/yum.repos.d/kernel-livepatch.repo:gpgcheck=1

If any repository has "gpgcheck=0" or "False", or if the option is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to verify the signature of packages from a repository prior to installation by setting the following option in the "/etc/yum.repos.d/[your_repo_name].repo" file:

gpgcheck=1

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

Internal Only - General

1.6 AZLX-23-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must be a vendor-supported release.

```
GROUP ID: V-273999
RULE ID: SV-273999r1155171
```

Rationale:

An operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software. Amazon Linux 2023 (AL2023) was released in March 2023 and will be supported until June 30, 2029.

Standard support ends June 30, 2027. Maintenance (security and critical fixes only) ends June 30, 2029.

To check the support status and dates of individual packages, use the following command:

```
$ sudo dnf supportinfo --pkg <packagename>
```

To get information on all currently installed packages, use:

```
$ sudo dnf supportinfo --show installed
```

Audit:

Verify Amazon Linux 2023 is a vendor-supported version with the following command:

```
$ cat /etc/amazon-linux-release
```

Amazon Linux release 2023.6.20250203 (Amazon Linux)

If the installed version of Amazon Linux 2023 is not supported, this is a finding.

Remediation:

Configure Amazon Linux 2023 to be a vendor supported release.

Upgrade to a supported version of Amazon Linux 2023.

Additional Information:

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c

Internal Only - General

- NIST SP 800-53 Revision 5::SI-2 c

Internal Only - General

1.7 AZLX-23-000135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 systemd-journald service must be enabled.

```
GROUP ID: V-274000
RULE ID: SV-274000r1119988
```

Rationale:

Failure to a known state can address safety or security in accordance with the mission/business needs of the organization. Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system.

Preserving operating system state information helps to facilitate operating system restart and return to the operational mode of the organization with least disruption to mission/business processes.

Audit:

Verify Amazon Linux 2023 is configured so that "systemd-journald" is active with the following command:

```
$ systemctl is-active systemd-journald
```

active

If the systemd-journald service is not active, this is a finding.

Remediation:

Configure Amazon Linux 2023 to enable the systemd-journald service with the following command:

```
$ sudo systemctl enable --now systemd-journald
```

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

1.8 AZLX-23-000200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must restrict access to the kernel message buffer.

```
GROUP ID: V-274001
RULE ID: SV-274001r1119991
```

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 nonprivileged user.

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000138-GPOS-00069

Audit:

Verify Amazon Linux 2023 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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

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

1.9 AZLX-23-000205 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must prevent kernel profiling by nonprivileged users.

```
GROUP ID: V-274002
RULE ID: SV-274002r1119994
```

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 nonprivileged user.

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000138-GPOS-00069

Audit:

Verify Amazon Linux 2023 is configured to prevent kernel profiling by nonprivileged 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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to prevent kernel profiling by nonprivileged users.

Add or edit the following line in a system configuration file, in the "/etc/sysctl.d/" directory:

kernel.perf_event_paranoid = 2

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

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

1.10 AZLX-23-000210 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must restrict exposed kernel pointer addresses access.

```
GROUP ID: V-274003
RULE ID: SV-274003r1119997
```

Rationale:

Exposing kernel pointers (through procfs or "seq_printf()") exposes kernel writeable structures, which may contain functions pointers. If a write vulnerability occurs in the kernel, allowing write access to any of this structure, the kernel can be compromised. This option disallows any program without the CAP_SYSLOG capability to get the addresses of kernel pointers by replacing them with "0".

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000433-GPOS-00192

Audit:

Verify Amazon Linux 2023 restricts exposed kernel pointer addresses access by validating the runtime status of the Amazon Linux 2023 kernel.kptr_restrict kernel parameter with the following command:

```
$ sudo sysctl kernel.kptr_restrict
```

kernel.kptr_restrict = 1

If "kernel.kptr_restrict" is not set to "1" or is missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 to restrict exposed kernel pointer addresses access.

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

kernel.kptr_restrict = 1

Reload settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```


Internal Only - General

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

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

1.11 AZLX-23-000215 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must disable access to network bpf system call from nonprivileged processes.

```
GROUP ID: V-274004
RULE ID: SV-274004r1120000
```

Rationale:

Loading and accessing the packet filters programs and maps using the bpf() system call has the potential of revealing sensitive information about the kernel state.

Audit:

Verify Amazon Linux 2023 prevents privilege escalation through the kernel by disabling access to the bpf system call 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.

Remediation:

Configure Amazon Linux 2023 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

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
```


Internal Only - General

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

Internal Only - General

1.12 AZLX-23-000220 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must restrict usage of ptrace to descendant processes.

```
GROUP ID: V-274005
RULE ID: SV-274005r1120003
```

Rationale:

Unrestricted usage of ptrace allows compromised binaries to run ptrace on other processes of the user. Like this, the attacker can steal sensitive information from the target processes (e.g., SSH sessions, web browser, etc.) without any additional assistance from the user (i.e., without resorting to phishing).

Audit:

Verify Amazon Linux 2023 restricts usage 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.

Remediation:

Configure Amazon Linux 2023 to restrict usage of ptrace to descendant processes by adding the following line to a file, in the "/etc/sysctl.d" directory:

kernel.yama.ptrace_scope = 1

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
```


Internal Only - General

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

Internal Only - General

1.13 AZLX-23-000225 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution.

```
GROUP ID: V-274006
RULE ID: SV-274006r1120006
```

Rationale:

ASLR makes it more difficult for an attacker to predict the location of attack code they have introduced into a process' address space during an attempt at exploitation. Additionally, ASLR makes it more difficult for an attacker to know the location of existing code to repurpose it using return oriented programming (ROP) techniques.

Audit:

Verify Amazon Linux 2023 is implementing ASLR with the following command:

```
$ sysctl kernel.randomize_va_space
```

kernel.randomize_va_space = 2

Check that the configuration files are present to enable this kernel parameter. Verify the configuration of the kernel.kptr_restrict kernel parameter with the following command:

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.randomize_va_space | tail -1
```

kernel.randomize_va_space = 2

If "kernel.randomize_va_space" is not set to "2" or is missing, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to enable ASLR to enhance memory protection.

Enable ASLR by setting the kernel parameter with the following command: echo 2 | sudo tee /proc/sys/kernel/randomize_va_space

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

kernel.randomize_va_space = 2

Reload settings from all system configuration files with the following command:

```
$ 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

1.14 AZLX-23-000300 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must not have the vsftpd package installed.

```
GROUP ID: V-274007
RULE ID: SV-274007r1120009
```

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 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 nonessential 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.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000095-GPOS-00049

Audit:

Verify Amazon Linux 2023 does not have the vsftpd package installed with the following command:

```
$ dnf list --installed vsftpd
```

Error: No matching Packages to list

If the "vsftpd" package is installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not have the vsftpd package installed with the following command:

```
$ sudo dnf -y remove vsftpd
```


Internal Only - General

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

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

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

1.15 AZLX-23-000305 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must not have the sendmail package installed.

```
GROUP ID: V-274008
RULE ID: SV-274008r1120012
```

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 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 nonessential 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.

Audit:

Verify Amazon Linux 2023 does not have the sendmail package installed with the following command:

```
$ dnf list --installed sendmail
```

Error: No matching Packages to list

If the "sendmail" package is installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not have the sendmail package installed with the following command:

```
$ sudo dnf -y 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

1.16 AZLX-23-000310 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must not have the nfs-utils package installed.

```
GROUP ID: V-274009
RULE ID: SV-274009r1120015
```

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 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 nonessential 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.

Audit:

Verify Amazon Linux 2023 does not have the nfs-utils package installed with the following command:

```
$ dnf list --installed nfs-utils
```

Error: No matching Packages to list

If the "nfs-utils" package is installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not have the nfs-utils package installed with the following command:

```
$ sudo dnf -y remove nfs-utils
```


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

1.17 AZLX-23-000315 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must not have the telnet-server package installed.

```
GROUP ID: V-274010
RULE ID: SV-274010r1120018
```

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 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 nonessential 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.

Audit:

Verify Amazon Linux 2023 does not have the telnet-server package installed with the following command:

```
$ dnf list --installed telnet-server
```

Error: No matching Packages to list

If the "telnet-server" package is installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not have the telnet-server package installed with the following command:

```
$ sudo dnf -y remove telnet-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

1.18 AZLX-23-000320 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must not have the gssproxy package installed.

```
GROUP ID: V-274011
RULE ID: SV-274011r1120021
```

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 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 nonessential 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.

Audit:

Verify Amazon Linux 2023 does not have the gssproxy package installed with the following command:

```
$ dnf list --installed gssproxy
```

Error: No matching Packages to list

If the "gssproxy" package is installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not have the gssproxy package installed.

The gssproxy package can be removed with the following command:

```
$ sudo dnf -y remove gssproxy
```


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

1.19 AZLX-23-001000 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the sudo package installed.

```
GROUP ID: V-274012
RULE ID: SV-274012r1120710
```

Rationale:

The "sudo" program is designed to allow a system administrator to give limited root privileges to users and log root activity. The basic philosophy is to give as few privileges as possible but still allow system users to get their work done.

Audit:

Verify Amazon Linux 2023 has the sudo package installed with the following command:

```
$ dnf list --installed sudo
```

Installed Packages sudo.x86_64 1.9.15-1.p5.amzn2023.0.1 @System

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

Remediation:

Configure Amazon Linux 2023 to have the sudo package installed with the following command:

```
$ sudo dnf install -y sudo
```

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

1.20 AZLX-23-001005 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must not be configured to bypass password requirements for privilege escalation.

```
GROUP ID: V-274013
RULE ID: SV-274013r1120027
```

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.

Audit:

Verify Amazon Linux 2023 is not configured to bypass password requirements for privilege escalation with the following command:

```
$ sudo grep pam_succeed_if /etc/pam.d/sudo
```

If any occurrences of "pam_succeed_if" are returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 to require users to supply a password for privilege escalation.

Remove any occurrences of "pam_succeed_if " in the "/etc/pam.d/sudo" file.

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

1.21 AZLX-23-001010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must require reauthentication when using the "sudo" command.

```
GROUP ID: V-274014
RULE ID: SV-274014r1120030
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

Audit:

Verify Amazon Linux 2023 requires reauthentication when using the "sudo" command to elevate privileges with the following command:

```
$ sudo grep -ir 'timestamp_timeout' /etc/sudoers /etc/sudoers.d/
```

/etc/sudoers:Defaults timestamp_timeout=0

If results are returned from more than one file location, 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.

Remediation:

Configure Amazon Linux 2023 to reauthenticate "sudo" commands after the specified timeout:

Add the following line to "/etc/sudoers" or a file in "/etc/sudoers.d":

Defaults timestamp_timeout=0

Additional Information:

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

1.22 AZLX-23-001015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must require users to reauthenticate for privilege escalation.

```
GROUP ID: V-274015
RULE ID: SV-274015r1120033
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

Audit:

Verify Amazon Linux 2023 requires users to reauthenticate for privilege escalation.

Ensure that "/etc/sudoers" has no occurrences of "!authenticate" with the following command:

```
$ sudo grep -ir '!authenticate' /etc/sudoers /etc/sudoers.d/
```

If any occurrences of "!authenticate" are returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not allow users to execute privileged actions without authenticating.

Remove any occurrence of "!authenticate" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

```
$ sudo sed -i '/\!authenticate/ s/^/# /g' /etc/sudoers /etc/sudoers.d/*
```

Additional Information:

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

1.23 AZLX-23-001020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must require users to provide a password for privilege escalation.

```
GROUP ID: V-274016
RULE ID: SV-274016r1120036
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

Audit:

Verify Amazon Linux 2023 requires users to provide a password for privilege escalation.

Ensure that "/etc/sudoers" has no occurrences of "NOPASSWD" with the following command:

```
$ sudo grep -ri nopasswd /etc/sudoers /etc/sudoers.d/
```

If any occurrences of "NOPASSWD" are returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 to not allow users to execute privileged actions without authenticating with a password.

Remove any occurrence of "NOPASSWD" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

```
$ sudo sed -i '/NOPASSWD/ s/^/# /g' /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

1.24 AZLX-23-001025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the audit package installed.

```
GROUP ID: V-274017
RULE ID: SV-274017r1120039
```

Rationale:

Successful incident response and auditing relies on timely, accurate system information and analysis to allow the organization to identify and respond to potential incidents in a proficient manner. If Amazon Linux 2023 does not provide the ability to centrally review Amazon Linux 2023 logs, forensic analysis is negatively impacted.

Segregation of logging data to multiple disparate computer systems is counterproductive and makes log analysis and log event alarming difficult to implement and manage, particularly when the system has multiple logging components writing to different locations or systems.

To support the centralized capability, Amazon Linux 2023 must be able to provide the information in a format that can be extracted and used, allowing the application performing the centralization of the log records to meet this requirement.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000042-GPOS-00021, 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-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, 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, SRG-OS-000055-GPOS-00026

Audit:

Verify Amazon Linux 2023 has the audit package installed with the following command:

```
$ dnf list --installed audit
```

Installed Packages audit.x86_64 3.0.6-1.amzn2023.0.2 @System

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

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that 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 dnf install -y audit
```

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

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-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.

Internal Only - General

- 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-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-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-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)

Internal Only - General

- 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-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-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-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.

Internal Only - General

- 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-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

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-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-000159 Use internal system clocks to generate time stamps for audit records.

- NIST SP 800-53::AU-8
- NIST SP 800-53A::AU-8.1
- NIST SP 800-53 Revision 4::AU-8 a
- NIST SP 800-53 Revision 5::AU-8 a

Internal Only - General

1.25 AZLX-23-001030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must produce audit records containing information to establish what type of events occurred.

```
GROUP ID: V-274018
RULE ID: SV-274018r1120042
```

Rationale:

Without establishing what type of events occurred, 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 Amazon Linux 2023 audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating 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-000062-GPOS-00031, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, 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, SRG-OS-000755-GPOS-00220

Audit:

Verify Amazon Linux 2023 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; preset: enabled) Active: active (running) since Wed 2024-01-131 12:56:56 EST; 1 weeks 0 days ago

If the audit service is not "active" and "running", this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the audit service to produce audit records containing the information needed to establish when 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

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

Internal Only - General

- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

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-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-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-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1

Internal Only - General

- 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-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-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-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.

Internal Only - General

- 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-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

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-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-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5::MA-3 (5)

Internal Only - General

1.26 AZLX-23-001035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audispd-plugins package must be installed.

```
GROUP ID: V-274019
RULE ID: SV-274019r1120045
```

Rationale:

The "audispd-plugins" package provides plugins for the real-time interface to the audit subsystem, "audispd". These plugins can, for example, relay events to remote machines or analyze events for suspicious behavior.

Audit:

Verify Amazon Linux 2023 has the audispd-plugins package installed with the following command:

```
$ sudo dnf list --installed audispd-plugins
```

Installed Packages audispd-plugins.x86_64 3.0.6-1.amzn2023.0.2 @amazonlinux

If the "audispd-plugins" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the audispd-plugins package installed.

Install the audispd-plugins package with the following command:

```
$ sudo dnf install -y audispd-plugins
```

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

1.27 AZLX-23-001040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the rsyslog package installed.

```
GROUP ID: V-274020
RULE ID: SV-274020r1155173
```

Rationale:

Successful incident response and auditing relies on timely, accurate system information and analysis allow the organization to identify and respond to potential incidents in a proficient manner. If Amazon Linux 2023 does not provide the ability to centrally review Amazon Linux 2023 logs, forensic analysis is negatively impacted.

Segregation of logging data to multiple disparate computer systems is counterproductive and makes log analysis and log event alarming difficult to implement and manage, particularly when the system has multiple logging components writing to different locations or systems.

To support the centralized capability, Amazon Linux 2023 must be able to provide the information in a format that can be extracted and used, allowing the application performing the centralization of the log records to meet this requirement.

Satisfies: SRG-OS-000051-GPOS-00024, SRG-OS-000479-GPOS-00224

Audit:

Verify Amazon Linux 2023 is configured to collect system failure events with the following command:

```
$ dnf list --installed rsyslog
```

Installed Packages rsyslog.x86_64 8.2204.0-3.amzn2023.0.4 @amazonlinux

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

Check that the log service is enabled with the following command:

systemctl is-enabled rsyslog enabled

If the command above returns "disabled", this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to monitor all remote access methods by installing rsyslog with the following command:

```
$ sudo dnf install -y rsyslog
```

Enable the log service with the following command:

```
$ sudo systemctl enable --now rsyslog
```

Additional Information:

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-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

1.28 AZLX-23-001045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must monitor remote access methods.

```
GROUP ID: V-274021
RULE ID: SV-274021r1120695
```

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.

Audit:

Verify Amazon Linux 2023 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
```

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

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

Remediation:

Configure Amazon Linux 2023 to monitor all remote access methods by installing rsyslog with the following command:

```
$ sudo yum install rsyslog
```

Then 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
```


Internal Only - General

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

1.29 AZLX-23-001050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the chrony package installed.

```
GROUP ID: V-274022
RULE ID: SV-274022r1120054
```

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.

Audit:

Verify Amazon Linux 2023 has the chrony package installed with the following command:

```
$ sudo dnf list --installed chrony
```

Installed Packages chrony.x86_64 4.3-1.amzn2023.0.5 @System

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

Remediation:

Configure Amazon Linux 2023 to have the chrony package installed.

The chrony package can be installed with the following command:

```
$ sudo dnf install -y chrony
```

Additional Information:

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)

Internal Only - General

1.30 AZLX-23-001055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 chronyd service must be enabled.

```
GROUP ID: V-274023
RULE ID: SV-274023r1120057
```

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.

Audit:

Verify Amazon Linux 2023 has the chronyd service set to active with the following command:

```
$ systemctl is-active chronyd
```

active

If the chronyd service is not active, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the chronyd service set to active with the following command:

```
$ sudo systemctl enable --now chronyd
```

Additional Information:

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)

Internal Only - General

1.31 AZLX-23-001060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the Advanced Intrusion Detection Environment (AIDE) package installed.

```
GROUP ID: V-274024
RULE ID: SV-274024r1120060
```

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.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000445-GPOS-00199, SRG-OS-000358-GPOS-00145

Audit:

Verify Amazon Linux 2023 has the AIDE package installed with the following command:

```
$ dnf list --installed aide
```

Installed Packages aide.x86_64 0.18.6-1.amzn2023.0.1 @amazonlinux

If AIDE is not installed, ask the system administrator (SA) 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:

Configure Amazon Linux 2023 to have the AIDE package installed.

Install AIDE with the following commands:

Install AIDE:

```
$ sudo dnf install -y aide
```

Initialize AIDE:

```
$ sudo /usr/sbin/aide --init
```

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:

2023-06-05 10:16:08 -0600 (AIDE 0.16) AIDE found NO differences between database and filesystem. Looks okay!!

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-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

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

Internal Only - General

1.32 AZLX-23-001065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must routinely check the baseline configuration for unauthorized changes and notify the system administrator when anomalies in the operation of any security functions are discovered.

```
GROUP ID: V-274025
RULE ID: SV-274025r1120723
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to Amazon Linux 2023. 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 Amazon Linux 2023. Amazon Linux 2023's information management officer (IMO)/information system security officer (ISSO) and system administrators (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.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000446-GPOS-00200, SRG-OS-000447-GPOS-00201

Internal Only - General

Audit:

Verify Amazon Linux 2023 routinely executes a file integrity scan for changes to the system baseline. The commands 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 Advanced Intrusion Detection Environment (AIDE) is installed on the system, use the following commands:

```
$ ls -al /etc/cron.daily | grep aide
```

-rwxr-xr-x 1 root root 29 Nov 22 2015 aide

```
$ sudo grep aide /etc/crontab /var/spool/cron/root
```

/etc/crontab: 30 04 * * * root usr/sbin/aide /var/spool/cron/root: 30 04 * * * root usr/sbin/aide

```
$ sudo more /etc/cron.daily/aide
```

#!/bin/bash /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily aide integrity check run" root@sysname.mil

If the file integrity application does not exist, or 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.

Remediation:

Configure Amazon Linux 2023 so that the file integrity tool runs automatically on the system at least weekly and notifies 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 email at the completion of the analysis.

```
$ sudo more /etc/cron.daily/aide
```

#!/bin/bash /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily aide integrity check run" root@sysname.mil

Internal Only - General

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

1.33 AZLX-23-001070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must use cryptographic mechanisms to protect the integrity of audit tools.

```
GROUP ID: V-274026
RULE ID: SV-274026r1120066
```

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.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000278-GPOS-00108

Internal Only - General

Audit:

Verify Amazon Linux 2023 is properly configured to protect the integrity of the Advanced Intrusion Detection Environment (AIDE) audit tools with the following command:

```
$ sudo grep /usr/sbin/au /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/augenrules
p+i+n+u+g+s+b+acl+xattrs+sha512

If AIDE is not installed, ask the system administrator (SA) how file integrity checks are performed on the system.

If any of the audit tools listed above do not have a corresponding line, ask the SA to indicate what cryptographic mechanisms are being used to protect the integrity of the audit tools.

If there is no evidence of integrity protection, this is a finding.

Remediation:

Configure Amazon Linux 2023 to protect the integrity of the AIDE audit tools.

Add or update the following lines to "/etc/aide.conf", to protect the integrity of the 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/augenrules
p+i+n+u+g+s+b+acl+xattrs+sha512

Internal Only - General

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

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

1.34 AZLX-23-001075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the firewalld package installed.

```
GROUP ID: V-274027
RULE ID: SV-274027r1120069
```

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, Amazon Linux 2023 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.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115, SRG-OS-000298-GPOS-00116, SRG-OS-000480-GPOS-00232, SRG-OS-000304-GPOS-00121

Audit:

Verify Amazon Linux 2023 has the firewalld package installed with the following command:

```
$ dnf list --installed firewalld
```

Installed Packages firewalld.noarch 1.2.3-1.amzn2023 @amazonlinux

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

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to have the firewalld package installed with the following command:

```
$ sudo dnf install -y firewalld
```

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

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)

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-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

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)

Internal Only - General

1.35 AZLX-23-001080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the firewalld servicew active.

```
GROUP ID: V-274028
RULE ID: SV-274028r1120072
```

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 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, Amazon Linux 2023 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.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115, SRG-OS-000298-GPOS-00116, SRG-OS-000480-GPOS-00232, SRG-OS-000304-GPOS-00121

Audit:

Verify Amazon Linux 2023 firewalld service is active with the following command:

```
$ systemctl is-active firewalld
```

active

If the "firewalld" service is not active, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to enable the firewalld service with the following command:

```
$ sudo systemctl enable --now firewalld
```

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

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)

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-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

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)

Internal Only - General

1.36 AZLX-23-001085 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must be configured to disable nonessential capabilities.

```
GROUP ID: V-274029
RULE ID: SV-274029r1120075
```

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 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 nonessential 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.

Audit:

Verify Amazon Linux 2023 is configured to disable nonessential capabilities.

Inspect the list of enabled firewall ports and verify they are configured correctly by running the following command:

```
$ sudo firewall-cmd --list-all
```

Ask the system administrator for the site or program Ports, Protocols, and Services Management Component Local Service Assessment (PPSM 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 Category Assurance List (CAL), or there are no firewall rules configured, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to allow approved settings and/or running services to comply with the PPSM CLSA for the site or program and the PPSM CAL.

To open a port for a service, configure firewalld using the following command:

```
$ sudo firewall-cmd --permanent --add-port=port_number/tcp
```

or

```
$ sudo firewall-cmd --permanent --add-service=service_name
```

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

1.37 AZLX-23-001090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-274030
RULE ID: SV-274030r1120078
```

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.

Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Audit:

Verify Amazon Linux 2023 manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of DoS attacks.

Verify nftables is configured to allow rate limits on any connection to the system with the following command:

```
$ sudo grep -i firewallbackend /etc/firewalld/firewalld.conf
```

FirewallBackend=nftables

Remediation:

Configure Amazon Linux 2023 to manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of DoS attacks.

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.

Internal Only - General

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)

Internal Only - General

1.38 AZLX-23-001095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the s-nail package installed.

```
GROUP ID: V-274031
RULE ID: SV-274031r1120081
```

Rationale:

The "s-nail" package provides the mail command required to allow sending email notifications of unauthorized configuration changes to designated personnel.

Audit:

Verify Amazon Linux 2023 has the "s-nail" package is installed on the system with the following command:

```
$ dnf list --installed s-nail
```

Installed Packages s-nail.x86_64 14.9.24-6.amzn2023 @amazonlinux

If the "s-nail" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the s-nail package installed with the following command:

```
$ sudo dnf install -y s-nail
```

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

1.39 AZLX-23-001105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the libreswan package installed.

```
GROUP ID: V-274032
RULE ID: SV-274032r1120084
```

Rationale:

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

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

FIPS 140-2/140-3 is the current standard for validating that mechanisms used to access cryptographic modules utilize 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 Amazon Linux 2023 has the libreswan package installed with the following command:

```
$ dnf list --installed libreswan
```

Installed Packages libreswan.x86_64 4.12-3.amzn2023.0.2 @amazonlinux

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

Remediation:

Configure Amazon Linux 2023 to have the libreswan package installed with the following command:

```
$ sudo dnf install -y libreswan
```


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

1.40 AZLX-23-001110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the policycoreutils package installed.

```
GROUP ID: V-274033
RULE ID: SV-274033r1120087
```

Rationale:

An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are 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. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For nonkernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries. Operating systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Audit:

Verify Amazon Linux 2023 has the policycoreutils package installed with the following command:

```
$ dnf list --installed policycoreutils
```

Installed Packages policycoreutils.x86_64 3.4-6.amzn2023.0.2 @System

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

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to have the policycoreutils package installed with the following command:

```
$ sudo dnf install -y 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

1.41 AZLX-23-001115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the pcsc-lite package installed.

```
GROUP ID: V-274034
RULE ID: SV-274034r1120090
```

Rationale:

The pcsc-lite package must be installed if it is to be available for multifactor authentication using smart cards.

Audit:

Verify Amazon Linux 2023 has the pcsc-lite package installed with the following command:

```
$ dnf list --installed pcsc-lite
```

Installed Packages pcsc-lite.x86_64 1.9.1-1.amzn2023.0.4 @amazonlinux

If the "pcsc-lite" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the pcsc-lite package installed with the following command:

```
$ sudo dnf install -y pcsc-lite
```

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)

Internal Only - General

1.42 AZLX-23-001120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the packages required for encrypting off-loaded audit logs installed.

```
GROUP ID: V-274035
RULE ID: SV-274035r1120093
```

Rationale:

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

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

FIPS 140-2/140-3 is the current standard for validating that mechanisms used to access cryptographic modules utilize 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 Amazon Linux 2023 has the rsyslog-openssl package installed with the following command:

```
$ dnf list --installed rsyslog-openssl
```

Installed Packages rsyslog-openssl.x86_64 8.2204.0-3.amzn2023.0.4 @amazonlinux

If the "rsyslog-openssl" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the rsyslog-openssl package installed with the following command:

```
$ sudo dnf install -y rsyslog-openssl
```


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

1.43 AZLX-23-001125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the opensc package installed.

```
GROUP ID: V-274036
RULE ID: SV-274036r1120096
```

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.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000376-GPOS-00161

Audit:

Verify Amazon Linux 2023 has the opensc package installed with the following command:

```
$ sudo dnf list --installed opensc
```

Installed Packages opensc.x86_64 0.24.0-1.amzn2023.0.4 @amazonlinux

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

Remediation:

Configure Amazon Linux 2023 to have the opensc package installed with the following command:

```
$ sudo dnf install -y opensc
```


Internal Only - General

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-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

1.44 AZLX-23-001130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the openssl-pkcs11 package installed.

```
GROUP ID: V-274037
RULE ID: SV-274037r1120099
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased. Multifactor authentication requires using two or more factors to achieve authentication. A privileged account is defined as an information system account with authorizations of a privileged user. The DOD Common Access Card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000376-GPOS-00161, SRG-OS-000377-GPOS-00162

Audit:

Verify Amazon Linux 2023 has the openssl-pkcs11 package installed with the following command:

```
$ dnf list --installed openssl-pkcs11
```

Installed Packages openssl-pkcs11.x86_64 0.4.12-3.amzn2023.0.1 @System

If the "openssl-pkcs11" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the openssl-pkcs11 package installed with the following command:

```
$ sudo dnf install -y openssl-pkcs11
```


Internal Only - General

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-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)

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)

Internal Only - General

1.45 AZLX-23-001180 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must have SSH installed.

```
GROUP ID: V-274038
RULE ID: SV-274038r1120102
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058, SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify Amazon Linux 2023 has the openssh-server package installed with the following command:

```
$ dnf list --installed openssh-server
```

Installed Packages openssh-server.x86_64 8.7p1-8.amzn2023.0.13 @amazonlinux

If the "openssh-server" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the openssh-server package installed with the following command:

```
$ sudo dnf install -y openssh-server
```


Internal Only - General

Additional Information:

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

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-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-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-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

1.46 AZLX-23-001185 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

```
GROUP ID: V-274039
RULE ID: SV-274039r1120105
```

Rationale:

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions that have common application in digital signatures, checksums, and message authentication codes.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to leverage transmission protection mechanisms such as TLS, SSL VPNs, or IPSec.

Satisfies: SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058, SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify Amazon Linux 2023 has "sshd" set to active with the following command:

```
$ systemctl is-active sshd
```

active

If the "sshd" service is not active, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to enable the sshd service run the following command:

```
$ sudo systemctl enable --now sshd
```

Additional Information:

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

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-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-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-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

1.47 AZLX-23-001195 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must have the crypto-policies package installed.

```
GROUP ID: V-274040
RULE ID: SV-274040r1120108
```

Rationale:

Centralized cryptographic policies simplify applying secure ciphers across an operating system and the applications that run on that operating system. Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000424-GPOS-00188

Audit:

Verify Amazon Linux 2023 crypto-policies package is installed with the following command:

```
$ dnf list --installed crypto-policies
```

Installed Packages crypto-policies.noarch 20240828-2.git626aa59.amzn2023.0.1 @System

If the "crypto-policies" package is not installed, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have the crypto-policies package installed with the following command:

```
$ sudo dnf install -y crypto-policies
```


Internal Only - General

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

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)

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)

Internal Only - General

1.48 AZLX-23-001200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 SSH server must be configured to use systemwide crypto policies.

```
GROUP ID: V-274041
RULE ID: SV-274041r1120111
```

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.

Audit:

Verify Amazon Linux 2023 employs systemwide crypto policies for SSH 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*include'
```

/etc/ssh/sshd_config:Include /etc/ssh/sshd_config.d/*.conf /etc/ssh/sshd_config.d/50-redhat.conf:Include /etc/crypto-policies/back-ends/opensshserver.config

If "Include /etc/ssh/sshd_config.d/*.conf" or "Include /etc/crypto-policies/back-ends/opensshserver.config" are not included in the system sshd config or the file /etc/ssh/sshd_config.d/50-redhat.conf is missing, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the SSH daemon uses systemwide crypto policies by running the following commands:

```
$ sudo dnf reinstall -y openssh-server
```

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

1.49 AZLX-23-001205 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 server must be configured to use only DOD-approved encryption ciphers employing FIPS 140-2/140-3 validated cryptographic hash algorithms to protect the confidentiality of SSH server connections.

```
GROUP ID: V-274042
RULE ID: SV-274042r1120114
```

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.

Amazon Server 2023 incorporates systemwide 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.

Audit:

Verify Amazon Linux 2023 SSH server is configured to use only ciphers employing FIPS 140-2/140-3 approved algorithms with the following command:

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

Ciphers aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr

If the cipher entries in the "opensshserver.config" file have any ciphers other than "aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr", or they are missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the SSH server uses only ciphers employing FIPS 140-2/140-3 approved algorithms.

Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS
```

Setting system policy to FIPS

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

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

1.50 AZLX-23-001210 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 SSH server must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-2/140-3 validated cryptographic hash algorithms to protect the confidentiality of SSH server connections.

```
GROUP ID: V-274043
RULE ID: SV-274043r1120117
```

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.

Amazon Linux 2023 incorporates systemwide 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.

Audit:

Verify Amazon Linux 2023 SSH server is configured to use only MACs employing FIPS 140-2/140-3 approved algorithms.

To verify the MACs in the systemwide SSH configuration file, use the following command:

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

MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512

If the MACs entries in the "opensshserver.config" file have any hashes other than "hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512", or they are missing or commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the SSH server uses only MACs employing FIPS 140-2/140-3 approved algorithms.

Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS
```

Setting system policy to FIPS

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

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

1.51 AZLX-23-001215 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 SSH daemon must not allow Generic Security Service Application Program Interface (GSSAPI) authentication.

```
GROUP ID: V-274044
RULE ID: SV-274044r1120120
```

Rationale:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system.

Audit:

Verify Amazon Linux 2023 is configured so that 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'
```

/etc/ssh/sshd_config.d/50-redhat.conf:GSSAPIAuthentication no

If the value is returned as "yes", the returned line is commented out, no output is returned, and the use of GSSAPI authentication has not been documented with the information system security officer (ISSO), this is a finding.

If the required value is not set, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the SSH daemon does not allow GSSAPI authentication.

Add or uncomment the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d" and set the value to "no":

GSSAPIAuthentication no

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

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


Internal Only - General

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

Internal Only - General

1.52 AZLX-23-001220 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 SSH daemon must not allow Kerberos authentication.

```
GROUP ID: V-274045
RULE ID: SV-274045r1120123
```

Rationale:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementations may be subject to exploitation.

Audit:

Verify Amazon Linux 2023 is configured so that the SSH daemon does not allow Kerberos authentication with the following command:

```
$ [ec2-user@ip-172-31-12-63 ~]$ sudo /usr/sbin/sshd -dd 2>&1 | awk
'/filename/ {print $4}' | tr -d '\r' | tr '\n' ' ' | xargs sudo grep -iH
'^\s*kerberosauthentication'
```

/etc/ssh/sshd_config.d/93-KerberosAuthentication.conf:KerberosAuthentication no

If the value is returned as "yes", the returned line is commented out, no output is returned, and the use of Kerberos authentication has not been documented with the information system security officer (ISSO), this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the SSH daemon does not allow Kerberos authentication.

Add the following line in "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d" or uncomment the line and set the value to "no":

KerberosAuthentication no

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

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


Internal Only - General

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

Internal Only - General

1.53 AZLX-23-001225 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must force a frequent session key renegotiation for SSH connections to the server.

```
GROUP ID: V-274046
RULE ID: SV-274046r1120126
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either 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, then logical means (cryptography) do not have to be employed, and vice versa.

Session key regeneration limits the chances of a session key becoming compromised.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000033-GPOS-00014, SRG-OS-000424-GPOS-00188

Audit:

Verify Amazon Linux 2023 is configured so that the SSH forces 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, is missing, or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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 or in a file in "/etc/ssh/sshd_config.d":

RekeyLimit 1G 1h

Restart the SSH daemon for the settings to take effect.

```
$ sudo systemctl restart 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-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-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)

Internal Only - General

1.54 AZLX-23-001230 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 SSHD must accept public key authentication.

```
GROUP ID: V-274047
RULE ID: SV-274047r1120129
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

1. Something a user knows (e.g., password/PIN);
2. Something a user has (e.g., cryptographic identification device, token); and
3. Something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

The DOD Common Access Card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Audit:

Verify Amazon Linux 2023 is configured so that the SSH daemon accepts public key encryption with the following command:

```
$ sudo grep -ir PubkeyAuthentication /etc/ssh/sshd_config
/etc/ssh/sshd_config.d/
```

/etc/ssh/sshd_config:#PubkeyAuthentication yes /etc/ssh/sshd_config.d/90-PubkeyAuth:PubkeyAuthentication yes

If "PubkeyAuthentication" is set to no, the line is commented out, or the line is missing, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to use public key authentication for SSHD by adding or modifying the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

PubkeyAuthentication yes

Restart the SSH daemon for the settings to take effect:

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

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)

Internal Only - General

1.55 AZLX-23-001235 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 SSHD must not allow blank passwords.

```
GROUP ID: V-274048
RULE ID: SV-274048r1120132
```

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 must never be used in operational environments.

Satisfies: SRG-OS-000106-GPOS-00053, SRG-OS-000480-GPOS-00229

Audit:

Verify Amazon Linux 2023 remote access using SSH prevents logging on with a blank password with the following command:

```
$ sudo grep -ir PermitEmptyPasswords /etc/ssh/sshd_config
/etc/ssh/sshd_config.d/
```

/etc/ssh/sshd_config:PermitEmptyPasswords no

If the "PermitEmptyPassword" keyword is set to "yes", is missing, or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to prevent SSH users from logging on with blank passwords.

Edit the following line in "etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d":

PermitEmptyPasswords no

Restart the SSH daemon for the settings to take effect:

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


Internal Only - General

Additional Information:

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-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

1.56 AZLX-23-001240 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must not permit direct logons to the root account using remote access via SSH.

```
GROUP ID: V-274049
RULE ID: SV-274049r1120747
```

Rationale:

To ensure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated. Additionally, an additional layer of security is gained by extending the policy of not logging directly on as root, even though the communications channel may be encrypted.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator are the Unix OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the Unix and Windows operating systems offer a "switch user" capability allowing users to authenticate with their individual credentials and, when needed, switch" to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on Amazon Linux 2023 without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

Audit:

Verify Amazon Linux 2023 remote access using SSH prevents users from logging on directly as "root" with the following command:

```
$ sudo grep -ir PermitRootLogin /etc/ssh/sshd_config /etc/ssh/sshd_config.d/
```

/etc/ssh/sshd_config:PermitRootLogin no

If the "PermitRootLogin" keyword is set to "yes", is missing, or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to prevent SSH users from logging on directly as root add or modify the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

PermitRootLogin no

Restart the SSH daemon for the settings to take effect:

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

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)

Internal Only - General

1.57 AZLX-23-001245 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must be configured so that all network connections associated with SSH traffic are terminated after 10 minutes of becoming unresponsive.

```
GROUP ID: V-274050
RULE ID: SV-274050r1120138
```

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. In addition, quickly terminating an idle 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 Amazon Linux 2023 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 Amazon Linux 2023 terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109, SRG-OS-000395-GPOS-00175

Audit:

Verify Amazon Linux 2023 has the "ClientAliveInterval" variable set to a value of "600" or less by performing 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'
```

/etc/ssh/sshd_config.d/91-ClientAliveInterval.conf:ClientAliveInterval 600

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

Internal Only - General

Remediation:

Configure Amazon Linux 2023 SSH server to terminate a user session automatically after the SSH client has been unresponsive for 10 minutes.

Note: This setting must be applied in conjunction with "ClientAliveCountMax 1" to function correctly.

Modify or append the following lines in the "/etc/ssh/sshd_config" or a dropfile in "/etc/ssh/sshd_config.d" file:

ClientAliveInterval 600

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

CCI-002891 Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (7)
- NIST SP 800-53 Revision 5::MA-4 (7)

Internal Only - General

1.58 AZLX-23-001250 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.

```
GROUP ID: V-274051
RULE ID: SV-274051r1120141
```

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. In addition, quickly terminating an idle 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 Amazon Linux 2023 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 Amazon Linux 2023 terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

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

Audit:

Verify Amazon Linux 2023 SSHD has the "ClientAliveCountMax" set to "1" by performing 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'
```

/etc/ssh/sshd_config.d/92-ClientAliveCountMax.conf:ClientAliveCountMax 1

If "ClientAliveCountMax" do not exist, is not set to a value of "1" in "/etc/ssh/sshd_config" or a dropfile in "/etc/ssh/sshd_config.d" , or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 SSHD to terminate a user session automatically after the SSH client has become unresponsive.

Note: This setting must be applied in conjunction with AZLX-23-000820 to function correctly.

Modify or append the following lines in the "/etc/ssh/sshd_config" file or a dropfile in "/etc/ssh/sshd_config.d":

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

1.59 AZLX-23-001255 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must enable the Pluggable Authentication Module (PAM) interface for SSHD.

```
GROUP ID: V-274052
RULE ID: SV-274052r1120144
```

Rationale:

If maintenance tools are used by unauthorized personnel, they may accidentally or intentionally damage or compromise the system. The act of managing systems and applications includes the ability to access sensitive application information, such as system configuration details, diagnostic information, user information, and potentially sensitive application data.

Some maintenance and test tools are either standalone devices with their own operating systems or are applications bundled with an operating system.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

Audit:

Verify Amazon Linux 2023 SSHD is configured to allow for the UsePAM interface 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*usepam'
```

/etc/ssh/sshd_config.d/50-redhat.conf:UsePAM yes

If the "UsePAM" keyword is set to "no", is missing, or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 SSHD to use the UsePAM interface.

Add or modify the following line in "/etc/ssh/sshd_config":

UsePAM yes

Restart the SSH daemon for the settings to take effect:

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

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

1.60 AZLX-23-001260 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must implement DOD-approved encryption in the OpenSSL package.

```
GROUP ID: V-274053
RULE ID: SV-274053r1120147
```

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.

Audit:

Verify Amazon Linux 2023 is configured so that the OpenSSL library uses only ciphers employing FIPS 140-2/140-3 approved algorithms with the following command:

```
$ 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.

Remediation:

Configure Amazon Linux 2023 OpenSSL library to use the system wide cryptographic policy.

Edit the "/etc/pki/tls/openssl.cnf" and add or modify the following line:

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

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

1.61 AZLX-23-001265 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must implement DOD-approved TLS encryption in the OpenSSL package.

```
GROUP ID: V-274054
RULE ID: SV-274054r1120150
```

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.

Audit:

Verify Amazon Linux 2023 is configured so that the OpenSSL library uses TLS 1.2 encryption or stronger with following command:

```
$ 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 Amazon Linux 2023 OpenSSL library to use only DOD-approved TLS encryption by editing the following line in the "/etc/crypto-policies/back-ends/opensslcnf.config" file:

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

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

1.62 AZLX-23-001270 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must implement a FIPS 140-2/140-3 compliant systemwide cryptographic policy.

```
GROUP ID: V-274055
RULE ID: SV-274055r1120153
```

Rationale:

Centralized cryptographic policies simplify applying secure ciphers across an operating system and the applications that run on that operating system. Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data.

Satisfies: SRG-OS-000120-GPOS-00061, SRG-OS-000396-GPOS-00176, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000424-GPOS-00188

Internal Only - General

Audit:

Verify Amazon Linux 2023 is set to use a FIPS 140-2/140-3 compliant systemwide cryptographic policy.

```
$ update-crypto-policies --show
```

FIPS

If the systemwide crypto policy is not set to "FIPS", this is a finding.

Inspect the contents of the REQUIRE.pmod file (if it exists) to verify only authorized modifications to the current policy are included with the following command:

```
$ cat /etc/crypto-policies/policies/modules/REQUIRE.pmod
```

Note: If subpolicies have been configured, they could be listed in a colon-separated list starting with FIPS as follows FIPS:<SUBPOLICY-NAME>:<SUBPOLICY-NAME>. This is not a finding.

If the AD-SUPPORT subpolicy module is included (e.g., "FIPS:AD-SUPPORT"), and Active Directory support is not documented as an operational requirement with the information system security officer (ISSO), this is a finding.

If the NO-ENFORCE-EMS subpolicy module is included (e.g., "FIPS:NO-ENFORCE-EMS"), and not enforcing EMS is not documented as an operational requirement with the ISSO, this is a finding.

Verify the current minimum crypto-policy configuration with the following commands:

```
$ grep -E 'rsa_size|hash' /etc/crypto-policies/state/CURRENT.pol
```

hash = SHA2-256 SHA2-384 SHA2-512 SHA2-224 SHA3-256 SHA3-384 SHA3-512 SHAKE-256 min_rsa_size = 2048

If the "hash" values do not include at least the following FIPS 140-2/140-3 compliant algorithms "SHA2-256 SHA2-384 SHA2-512 SHA2-224 SHA3-256 SHA3-384 SHA3-512 SHAKE-256", this is a finding.

If there are algorithms that include "SHA1" or a hash value less than "256" this is a finding.

If the "min_rsa_size" is not set to a value of at least 2048, this is a finding.

If these commands do not return any output, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to use a FIPS 140-2/140-3 compliant systemwide cryptographic policy.

Create subpolicies for enhancements to the systemwide crypto-policy with the following commands:

Create or edit the SCOPES-AND-WILDCARDS policy module in a text editor and insert options that modify the systemwide cryptographic policy as follows:

```
$ sudo vi /etc/crypto-policies/policies/modules/SCOPES-AND-WILDCARDS.pmod
```

Add the following lines to the policy:

Disable CHACHA20-POLY1305 for the TLS protocol (OpenSSL, GnuTLS, NSS, and OpenJDK)

cipher@TLS = -CHACHA20-POLY1305

Disable all CBC mode ciphers for the SSH protocol (libssh and OpenSSH)

cipher@SSH = -*-CBC

Create or edit the OPENSSH-SUBPOLICY module in a text editor and insert options that modify the systemwide crypto-policy as follows:

```
$ sudo vi /etc/crypto-policies/policies/modules/OPENSSH-SUBPOLICY.pmod
```

Add the following lines to the policy:

Define ciphers for OpenSSH

cipher@SSH=AES-256-GCM AES-128-GCM AES-256-CTR AES-128-CTR

Define MACs for OpenSSH

mac@SSH=HMAC-SHA2-512 HMAC-SHA2-256

Create or edit the REQUIRE.pmod file and add the following lines to include the subpolicies in the FIPS configuration with the following command:

```
$ sudo vi /etc/crypto-policies/policies/modules/REQUIRE.pmod
```

Add the following lines to REQUIRE.pmod: @OPENSSH-SUBPOLICY @SCOPES-AND-WILDCARDS

Apply the policy enhancements to the FIPS systemwide cryptographic policy level with the following command:

```
$ sudo update-crypto-policies --set FIPS
```

Note: If additional subpolicies are being employed, they should be added to the REQUIRE.pmod as well. REQUIRE.pmod is included in the systemwide crypto-policy when it is set.

Internal Only - General

To make the cryptographic settings effective for already running services and applications, restart the system:

```
$ sudo reboot
```

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

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

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)

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)

Internal Only - General

1.63 AZLX-23-001275 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must implement DOD-approved encryption to protect the confidentiality of remote access sessions.

```
GROUP ID: V-274056
RULE ID: SV-274056r1120156
```

Rationale:

Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session.

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.

Encryption provides a means to secure the remote connection to prevent unauthorized access to the data traversing the remote access connection (e.g., RDP), thereby providing a degree of confidentiality. The encryption strength of a mechanism is selected based on the security categorization of the information.

Audit:

Verify Amazon Linux 2023 is configured so that the SSH server uses only ciphers employing FIPS 140-2/140-3 approved algorithms with the following command:

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

Ciphers aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr

If the cipher entries in the "opensshserver.config" file have any ciphers other than "aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr", they are missing, or commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 SSH server to use only ciphers employing FIPS 140-2/140-3 approved algorithms by updating the "/etc/crypto-policies/back-ends/opensshserver.config" file with the following line:

Ciphers aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr

A reboot is required 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)

Internal Only - General

1.64 AZLX-23-001280 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must enable FIPS mode.

```
GROUP ID: V-274057
RULE ID: SV-274057r1120159
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. Amazon Linux 2023 must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000125-GPOS-00065, SRG-OS-000396-GPOS-00176, SRG-OS-000423-GPOS-00187, SRG-OS-000478-GPOS-00223

Audit:

Verify Amazon Linux 2023 is in FIPS mode with the following command:

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

FIPS mode is enabled.

If FIPS mode is not enabled, this is a finding.

Remediation:

Configure Amazon Linux 2023 to implement FIPS mode with the following commands:

```
$ 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-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

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

1.65 AZLX-23-001285 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 crypto policy must not be overridden.

```
GROUP ID: V-274058
RULE ID: SV-274058r1120162
```

Rationale:

Centralized cryptographic policies simplify applying secure ciphers across an operating system and the applications that run on that operating system. Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000424-GPOS-00188, SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify Amazon Linux 2023 custom crypto policies are loaded correctly with the following command:

```
$ ls -l /etc/crypto-policies/back-ends/
```

lrwxrwxrwx. 1 root root 40 Mar 7 19:22 bind.config -> /usr/share/crypto-policies/FIPS/bind.txt lrwxrwxrwx. 1 root root 42 Mar 7 19:22 gnutls.config -> /usr/share/crypto-policies/FIPS/gnutls.txt lrwxrwxrwx. 1 root root 40 Mar 7 19:22 java.config -> /usr/share/crypto-policies/FIPS/java.txt lrwxrwxrwx. 1 root root 46 Mar 7 19:22 javasystem.config -> /usr/share/crypto-policies/FIPS/javasystem.txt lrwxrwxrwx. 1 root root 40 Mar 7 19:22 krb5.config -> /usr/share/crypto-policies/FIPS/krb5.txt lrwxrwxrwx. 1 root root 45 Mar 7 19:22 libreswan.config -> /usr/share/crypto-policies/FIPS/libreswan.txt lrwxrwxrwx. 1 root root 42 Mar 7 19:22 libssh.config -> /usr/share/crypto-policies/FIPS/libssh.txt -rw-r--r--. 1 root root 398 Mar 7 19:22 nss.config lrwxrwxrwx. 1 root root 43 Mar 7 19:22 openssh.config -> /usr/share/crypto-policies/FIPS/openssh.txt lrwxrwxrwx. 1 root root 49 Mar 7 19:22 opensshserver.config -> /usr/share/crypto-policies/FIPS/opensshserver.txt lrwxrwxrwx. 1 root root 43 Mar 7 19:22 openssl.config -> /usr/share/crypto-policies/FIPS/openssl.txt lrwxrwxrwx. 1 root root 48 Mar 7 19:22 openssl_fips.config -> /usr/share/crypto-policies/FIPS/openssl_fips.txt lrwxrwxrwx. 1 root root 46 Mar 7 19:22 opensslcnf.config -> /usr/share/crypto-policies/FIPS/opensslcnf.txt

If the paths do not point to the respective files under /usr/share/crypto-policies/FIPS path, this is a finding. Note: nss.config must not be hyperlinked.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to correctly implement the systemwide cryptographic policies by reinstalling the crypto-policies package contents.

Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS
```

Setting system policy to FIPS

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

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)

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-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)

Internal Only - General

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

1.66 AZLX-23-001290 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enable certificate-based smart card authentication.

```
GROUP ID: V-274059
RULE ID: SV-274059r1120165
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased. Multifactor authentication requires using two or more factors to achieve authentication. A privileged account is defined as an information system account with authorizations of a privileged user. The DOD Common Access Card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000705-GPOS-00150

Audit:

Note: If the system administrator demonstrates the use of an approved alternate multifactor authentication method, this requirement is not applicable.

Verify Amazon Linux 2023 has smart cards enabled in System Security Services Daemon (SSSD), run the following command:

```
$ sudo grep -ir pam_cert_auth /etc/sssd/sssd.conf /etc/sssd/conf.d/
```

/etc/sssd/sssd.conf:pam_cert_auth = True

If "pam_cert_auth" is not set to "True", the line is commented out, or the line is missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have smart cards enabled in SSSD.

Edit the file "/etc/sssd/sssd.conf" or a configuration file in "/etc/sssd/conf.d" and add or edit the following line:

pam_cert_auth = True

Internal Only - General

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)

Internal Only - General

1.67 AZLX-23-001295 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must map the authenticated identity to the user or group account for PKI-based authentication.

```
GROUP ID: V-274060
RULE ID: SV-274060r1120168
```

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.

Audit:

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

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:

```
$ sudo find /etc/sssd/sssd.conf /etc/sssd/conf.d/ -type f -exec cat {} \;
```

[sssd] config_file_version = 2 services = pam, sudo, ssh domains = testing.test

[pam] pam_cert_auth = True offline_credentials_expiration = 1

[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, ask the SA to indicate how certificates are mapped to accounts. If there is no evidence of certificate mapping, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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

1.68 AZLX-23-001300 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must implement certificate status checking for multifactor authentication.

```
GROUP ID: V-274061
RULE ID: SV-274061r1120171
```

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.

Amazon Linux 2023 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:

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

Verify Amazon Linux 2023 implements Online Certificate Status Protocol (OCSP) and is using the proper digest value on the system with the following command:

```
$ sudo grep -ir certificate_verification /etc/sssd/sssd.conf
/etc/sssd/conf.d/ | grep -v "^#"
```

certificate_verification = ocsp_dgst=sha512

If the certificate_verification line is missing from the [sssd] section, or is missing "ocsp_dgst=sha512", ask the administrator to indicate what type of multifactor authentication is being utilized 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 Amazon Linux 2023 to implement certificate status checking for multifactor authentication.

Review the "/etc/sssd/conf.d/certificate_verification.conf" file to determine if the system is configured to prevent OCSP or certificate verification.

Add the following line to the "/etc/sssd/conf.d/certificate_verification.conf" file:

certificate_verification = ocsp_dgst=sha512

Set the correct ownership and permissions on the "/etc/sssd/conf.d/certificate_verification.conf" file by running these commands:

```
$ sudo chown root:root "/etc/sssd/conf.d/certificate_verification.conf"
$ sudo chmod 600 "/etc/sssd/conf.d/certificate_verification.conf"
```

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)

Internal Only - General

1.69 AZLX-23-001305 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must prohibit the use of cached authenticators after one day.

```
GROUP ID: V-274062
RULE ID: SV-274062r1120174
```

Rationale:

If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

Audit:

Verify Amazon Linux 2023 is configured so that the System Security Services Daemon (SSSD) prohibits the use of cached authentications after one day.

Note: Cached authentication settings should be configured even if smart card authentication is not used on the system.

Check that SSSD allows cached authentications with the following command:

```
$ sudo grep -ir cache_credentials /etc/sssd/sssd.conf /etc/sssd/conf.d/
```

/etc/sssd/sssd.conf:cache_credentials = true

If "cache_credentials" is set to "false" or 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/
```

/etc/sssd/sssd.conf:offline_credentials_expiration = 1

If "offline_credentials_expiration" is not set to a value of "1", this is a finding.

Remediation:

Configure Amazon Linux 2023 SSSD service 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

Internal Only - General

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

1.70 AZLX-23-001310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

```
GROUP ID: V-274063
RULE ID: SV-274063r1120712
```

Rationale:

Without path validation, an informed trust decision by the relying party cannot be made 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-000775-GPOS-00230, SRG-OS-000384-GPOS-00167, SRG-OS-000403-GPOS-00182

Internal Only - General

Audit:

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

Verify Amazon Linux 2023 for PKI-based authentication has valid certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

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 and installed in the /etc/sssd/pki/sssd_auth_ca_db.pem location, this is a finding.

Remediation:

Configure Amazon Linux 2023 to have valid certificates by using AWS Certificate Manager (ACM) or another certificate manager to manage SSL/TLS certificates.

In the AWS Management Console, request or import the necessary SSL/TLS certificates into ACM.

ACM will handle the certificate lifecycle management, including validation and trust chain establishment.

Internal Only - General

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-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5::SC-17 b

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-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

Internal Only - General

1.71 AZLX-23-001315 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023, for PKI-based authentication, must enforce authorized access to the corresponding private key.

```
GROUP ID: V-274064
RULE ID: SV-274064r1120180
```

Rationale:

If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and nonrepudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Audit:

Verify Amazon Linux 2023 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:

Configure Amazon Linux 2023 SSH private key files to have a passcode.

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

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


Internal Only - General

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

1.72 AZLX-23-002000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system.

```
GROUP ID: V-274065
RULE ID: SV-274065r1120699
```

Rationale:

Display of a standardized and approved use notification before granting access to Amazon Linux 2023 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.

Internal Only - General

-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."
```

Audit:

Verify Amazon Linux 2023 displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the system over any publicly accessible connection.

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

```
$ more /etc/issue
```

"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 logon banner or the banner text does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via the ssh.

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."

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

Internal Only - General

1.73 AZLX-23-002005 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system via a SSH logon.

```
GROUP ID: V-274066
RULE ID: SV-274066r1120186
```

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible 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.

Internal Only - General

-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."
```

Audit:

Verify Amazon Linux 2023 displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the system from any SSH connection.

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'
```

/etc/ssh/sshd_config.d/80-bannerPointer.conf: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.

Remediation:

Configure Amazon Linux 2023 to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via ssh.

Edit the "etc/ssh/sshd_config" file or a file in "/etc/ssh/sshd_config.d" 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

Internal Only - General

Additional Information:

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

1.74 AZLX-23-002015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must allocate audit record storage capacity to store at least one week's worth of audit records, when audit records are not immediately sent to a central audit record storage facility.

```
GROUP ID: V-274067
RULE ID: SV-274067r1120653
```

Rationale:

To ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems must be able to allocate audit record storage capacity.

Audit:

Verify Amazon Linux 2023 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.

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.

Determine which partition the audit records are being written to with the following command:

```
$ sudo grep log_file /etc/audit/auditd.conf
```

log_file = /var/log/audit/audit.log

Check the size of the partition that audit records are written to with the following command and verify whether it is sufficiently large:

df -h /var/log/audit/

/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to provide adequate storage for at least one-week of audit logs when audit records are not immediately sent to a central audit record storage facility.

If the storage partition is not large enough for at least one week of audit logs, then either:

1. Resize the partition to ensure there is enough storage capacity.
2. Create a new partition for the audit logs.

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

1.75 AZLX-23-002020 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

Amazon Linux 2023 must use a separate file system for the system audit data path.

```
GROUP ID: V-274068
RULE ID: SV-274068r1120192
```

Rationale:

Placing "/var/log/audit" in its own partition enables better separation between audit files and other system files and helps ensure that auditing cannot be halted due to the partition running out of space.

Audit:

Verify Amazon Linux 2023 has a separate file system/partition 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.

```
$ mount | grep /var/log/audit
```

UUID=2efb2979-45ac-82d7-0ae632d11f51 on /var/log/home type xfs (rw,realtime,seclabel,attr2,inode64)

Remediation:

Configure Amazon Linux 2023 to have a separate file system/partition for the system audit data path.

Migrate the system audit data path onto a separate partition.

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

1.76 AZLX-23-002025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must label all off-loaded audit logs before sending them to the central log server.

```
GROUP ID: V-274069
RULE ID: SV-274069r1120195
```

Rationale:

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.

Audit:

Verify Amazon Linux 2023 is configured so that the Audit Daemon labels all off-loaded 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:

Configure Amazon Linux 2023 to be configured so that the Audit Daemon labels all off-loaded audit logs.

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.

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

1.77 AZLX-23-002030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must take appropriate action when the internal event queue is full.

```
GROUP ID: V-274070
RULE ID: SV-274070r1120198
```

Rationale:

The audit system should have an action setup in the event the internal event queue becomes full so that no data is lost. Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Audit:

Verify Amazon Linux 2023 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", "halt" or the line is commented out, ask the system administrator (SA) to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media takes appropriate action if the internal event queue becomes full, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the audit system takes an appropriate action when the internal event queue is full.

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

1.78 AZLX-23-002035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-274071
RULE ID: SV-274071r1120201
```

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 Amazon Linux 2023 takes action 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 /etc/audit/auditd.conf
```

space_left = 25%

If the value of the "space_left" keyword is not set to 25 percent of the storage volume allocated to audit logs, or if the line is commented out, ask the system administrator (SA) to indicate how the system is providing real-time alerts to the SA and information system security officer (ISSO). If the "space_left" value is not configured to the correct value, this is a finding.

Remediation:

Configure Amazon Linux 2023 to take action when the audit log storage volume reaches 75 percent of the maximum storage capacity.

Edit /etc/audit/auditd.conf and ensure the parameter "space_left = 25" is configured.

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

1.79 AZLX-23-002040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 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-274072
RULE ID: SV-274072r1120204
```

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 Amazon Linux 2023 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 SA 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 Amazon Linux 2023 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

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

1.80 AZLX-23-002045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must take action when allocated audit record storage volume reaches 95 percent of the audit record storage capacity.

```
GROUP ID: V-274073
RULE ID: SV-274073r1120207
```

Rationale:

If action is not taken when storage volume reaches 95 percent utilization, the auditing system may fail when the storage volume reaches capacity.

Audit:

Verify Amazon Linux 2023 takes action when allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep -w admin_space_left /etc/audit/auditd.conf
```

admin_space_left = 5%

If the value of the "admin_space_left" keyword is not set to 5 percent of the storage volume allocated to audit logs, or if the line is commented out, ask the system administrator (SA) to indicate how the system is taking action if the allocated storage is about to reach capacity. If the "space_left" value is not configured to the correct value, this is a finding.

Remediation:

Configure Amazon Linux 2023 to initiate an action when allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

admin_space_left = 5%

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

1.81 AZLX-23-002050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must take action when allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-274074
RULE ID: SV-274074r1120210
```

Rationale:

If action is not taken when storage volume reaches 95 percent utilization, the auditing system may fail when the storage volume reaches capacity.

Audit:

Verify Amazon Linux 2023 is configured to take action in the event of allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep admin_space_left_action /etc/audit/auditd.conf
```

admin_space_left_action = single

If the value of the "admin_space_left_action" is not set to "single", or if the line is commented out, ask the system administrator (SA) to indicate how the system is providing real-time alerts to the SA and information system security officer (ISSO).

If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the auditd service takes action in the event of allocated audit record storage volume reaching 95 percent of the repository maximum audit record storage capacity.

Edit the following line in "/etc/audit/auditd.conf" to ensure that the system is forced into single user mode in the event the audit record storage volume is about to reach maximum capacity:

admin_space_left_action = single

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

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

1.82 AZLX-23-002055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must immediately notify the system administrator (SA) and information system security officer (ISSO), at a minimum, of an audit processing failure event.

```
GROUP ID: V-274075
RULE ID: SV-274075r1120700
```

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 Amazon Linux 2023 is configured to notify the SA and/or ISSO (at a minimum) 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 Amazon Linux 2023 to that the auditd service notifies 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

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

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

1.83 AZLX-23-002060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must be configured to off-load audit records onto a different system from the system being audited via syslog.

```
GROUP ID: V-274076
RULE ID: SV-274076r1120216
```

Rationale:

The auditd service does not include the ability to send audit records to a centralized server for management directly. However, it can use a plug-in for audit event multiplexor (audispd) to pass audit records to the local syslog server.

Audit:

Verify Amazon Linux 2023 is configured use the audisp-remote syslog service with the following command:

```
$ sudo grep active /etc/audit/plugins.d/syslog.conf
```

active = yes

If the "active" keyword does not have a value of "yes", the line is commented out, or the line is missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 to use the audisp-remote syslog service.

Edit the /etc/audit/plugins.d/syslog.conf file and add or update the "active" option:

active = yes

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

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

1.84 AZLX-23-002065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must authenticate the remote logging server for off-loading audit logs via rsyslog.

```
GROUP ID: V-274077
RULE ID: SV-274077r1120219
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Audit:

Verify Amazon Linux 2023 authenticates the remote logging server for off-loading 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 (SA) to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.

Remediation:

Configure Amazon Linux 2023 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

1.85 AZLX-23-002070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited via rsyslog.

```
GROUP ID: V-274078
RULE ID: SV-274078r1120222
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Audit:

Verify Amazon Linux 2023 encrypts audit records off-loaded onto a different system or media from the system being audited via rsyslog with the following command:

```
$ 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.

Remediation:

Configure Amazon Linux 2023 to encrypt off-loaded audit records via rsyslog by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

$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

1.86 AZLX-23-002075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must encrypt via the gtls driver the transfer of audit records off-loaded onto a different system or media from the system being audited via rsyslog.

```
GROUP ID: V-274079
RULE ID: SV-274079r1120724
```

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.

Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (a secure communications library implementing the SSL, TLS, and DTLS protocols) creates a method to securely encrypt and off-load auditing.

Audit:

Verify Amazon Linux 2023 uses the gtls driver to encrypt audit records off-loaded onto a different system or media from the system being audited with the following command:

```
$ sudo grep -i '$DefaultNetstreamDriver' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
```

/etc/rsyslog.conf:$DefaultNetstreamDriver ossl

If the value of the "$DefaultNetstreamDriver" option is not set to "ossl" or the line is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to use the ossl driver to encrypt offloaded audit records by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

$DefaultNetstreamDriver ossl

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

1.87 AZLX-23-002080 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Amazon Linux 2023 must be configured to off-load audit records onto a different system from the system being audited via syslog.

```
GROUP ID: V-274080
RULE ID: SV-274080r1120228
```

Rationale:

The auditd service does not include the ability to send audit records to a centralized server for management directly. However, it can use a plug-in for audit event multiplexor (audispd) to pass audit records to the local syslog server.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify Amazon Linux 2023 off-loads audit records onto a different system with the following command:

```
$ more /etc/systemd/journal-upload.conf
```

[Upload] URL=192.168.21.2 ServerKeyFile=/etc/ssl/private/journal-upload.pem ServerCertificateFile=/etc/ssl/certs/journal-upload.pem TrustedCertificateFile=/etc/ssl/ca/trusted.pem

If all of the entries do not have values, are commented out, or are missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 to off-load audit records onto a different system or media from the system being audited.

If using systemd-journal-upload: Edit "/etc/systemd/journal-upload.conf" with the appropriate configuration:

[Upload] URL=https://[server.domain]:[port]

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

1.88 AZLX-23-002085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.

```
GROUP ID: V-274081
RULE ID: SV-274081r1120231
```

Rationale:

The actions taken by system administrators must be audited to keep a record of what was executed on the system, as well as for accountability purposes. Editing the sudoers file may be sign of an attacker trying to establish persistent methods to a system, auditing the editing of the sudoers files mitigates this risk.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers" with the following command:

```
$ sudo auditctl -l | grep '/etc/sudoers[^.]'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.89 AZLX-23-002090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.d/ directory.

```
GROUP ID: V-274082
RULE ID: SV-274082r1120234
```

Rationale:

The actions taken by system administrators must be audited to keep a record of what was executed on the system, as well as for accountability purposes. Editing the sudoers file may be sign of an attacker trying to establish persistent methods to a system, auditing the editing of the sudoers files mitigates this risk.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/" with the following command:

```
$ sudo auditctl -l | grep /etc/sudoers.d
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.90 AZLX-23-002095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

```
GROUP ID: V-274083
RULE ID: SV-274083r1120237
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications must be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/group)'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.91 AZLX-23-002100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

```
GROUP ID: V-274084
RULE ID: SV-274084r1120240
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications must be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/gshadow)'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.92 AZLX-23-002105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

```
GROUP ID: V-274085
RULE ID: SV-274085r1120243
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications must be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/security/opasswd)'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.93 AZLX-23-002110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit uses of the "execve" system call.

```
GROUP ID: V-274086
RULE ID: SV-274086r1120246
```

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 Amazon Linux 2023 is configured to audit the execution of the "execve" system call with the following command:

```
$ sudo auditctl -l | grep execve
```

-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k execpriv

-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k execpriv

If the command does not return all lines, or the lines are commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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=b64 -S execve -C uid!=euid -F euid=0 -k execpriv

-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k execpriv

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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

1.94 AZLX-23-002115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the chmod, fchmod, and fchmodat system calls.

```
GROUP ID: V-274087
RULE ID: SV-274087r1120249
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "chmod", "fchmod", and "fchmodat" system calls with the following command:

```
$ sudo auditctl -l | grep chmod
```

-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -k perm_mod

If the command does not return the expected line, or the line is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records upon successful/unsuccessful attempts to use the "chmod", "fchmod", and "fchmodat" syscalls.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -k perm_mod

To load the rule to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.95 AZLX-23-002120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the chown, fchown, fchownat, and lchown system calls.

```
GROUP ID: V-274088
RULE ID: SV-274088r1120252
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "chown", "fchown", "fchownat", and "lchown" system calls with the following command:

```
$ sudo auditctl -l | grep chown
```

-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F auid!=unset -k perm_mod

If the command does not return the expected line, or the line is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records upon successful/unsuccessful attempts to use the "chown", "fchown", "fchownat", and "lchown" system calls.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F auid!=unset -k perm_mod

To load the rule to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.96 AZLX-23-002125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr system calls.

```
GROUP ID: V-274089
RULE ID: SV-274089r1120255
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00216, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Internal Only - General

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls with the following command:

```
$ sudo auditctl -l | grep xattr
```

-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=b64 -S setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0 -k perm_mod

If the audit rules are not defined for the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls, or any of the lines returned are commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 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=b64 -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=0 -k perm_mod

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```


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-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-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

1.97 AZLX-23-002130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the truncate, ftruncate, creat, open, openat, and open_by_handle_at system calls.

```
GROUP ID: V-274090
RULE ID: SV-274090r1120258
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Internal Only - General

Audit:

Verify Amazon Linux 2023 is configured to audit successful/unsuccessful attempts to use the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls with the following command:

```
$ sudo auditctl -l | grep 'open\|truncate\|creat'
```

-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=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.

Remediation:

Configure Amazon Linux 2023 to generate an audit event for any successful/unsuccessful 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=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=b64 -S truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -k perm_access

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```


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-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-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

1.98 AZLX-23-002135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the init_module and finit_module system calls.

```
GROUP ID: V-274091
RULE ID: SV-274091r1120261
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "init_module" and "finit_module" system calls with the following command:

```
$ sudo auditctl -l | grep init_module
```

-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F auid!=unset -k module_chng

If audit rule is not defined for the "delete_module" system call, or the line returned is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate an audit event for any successful/unsuccessful use of the "init_module" and "finit_module" system calls by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F auid!=unset -k module_chng

To load the rule to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.99 AZLX-23-002140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the create_module system call.

```
GROUP ID: V-274092
RULE ID: SV-274092r1120264
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify Amazon Linux 2023 generates audit records when successful/unsuccessful attempts to use the "create_module" syscall occur with the following command:

```
$ sudo auditctl -l | grep "create_module"
```

-a always,exit -F arch=b64 -S create_module -F auid>=1000 -F auid!=-1 -F key=module-change

If audit rule is not defined for the "create_module" syscall, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records when successful/unsuccessful attempts to use the "create_module" syscall occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F arch=b64 -S create_module -F auid>=1000 -F auid!=unset -k module-change

To load the rule to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.100 AZLX-23-002145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the kmod command.

```
GROUP ID: V-274093
RULE ID: SV-274093r1120267
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify Amazon Linux 2023 generates audit records when successful/unsuccessful attempts to use the "kmod" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo auditctl -l | grep kmod
```

-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -k modules

If the command does not return a line, or the line is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records upon successful/unsuccessful attempts to use the "kmod" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -k modules

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.101 AZLX-23-002150 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the rename, unlink, rmdir, renameat, and unlinkat system calls.

```
GROUP ID: V-274094
RULE ID: SV-274094r1120270
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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, SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00211, SRG-OS-000468-GPOS-00212

Audit:

Verify Amazon Linux 2023 is configured to audit successful/unsuccessful attempts to use the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls with the following command:

```
$ sudo auditctl -l | grep 'rename\|unlink\|rmdir'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate an audit event for any successful/unsuccessful use of the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

-a always,exit -F arch=b64 -S rename,unlink,rmdir,renameat,unlinkat -F auid>=1000 -F auid!=unset -k delete

To load the rule to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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

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

1.102 AZLX-23-002155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the chcon command.

```
GROUP ID: V-274095
RULE ID: SV-274095r1120273
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account 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 system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls 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-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "chcon" command with the following command:

```
$ sudo auditctl -l | grep chcon
```

-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset -k perm_mod

If the command does not return a line, or the line is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records upon successful/unsuccessful attempts to use the "chcon" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset -k perm_mod

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.103 AZLX-23-002160 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /var/log/faillock.

```
GROUP ID: V-274096
RULE ID: SV-274096r1120276
```

Rationale:

Without generating audit records 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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/faillock" with the following command:

```
$ sudo auditctl -l | grep /var/log/faillock
```

-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 Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/faillock".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

-w /var/log/faillock -p wa -k logins

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```


Internal Only - General

Additional Information:

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-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

1.104 AZLX-23-002165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /var/log/lastlog.

```
GROUP ID: V-274097
RULE ID: SV-274097r1120279
```

Rationale:

Without generating audit records 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.

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, SRG-OS-000470-GPOS-00214

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/lastlog" with the following command:

```
$ sudo auditctl -l | grep /var/log/lastlog
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/lastlog".

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

-w /var/log/lastlog -p wa -k logins

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.105 AZLX-23-002175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the init command.

```
GROUP ID: V-274098
RULE ID: SV-274098r1120282
```

Rationale:

Misuse of the init command may cause availability issues for the system.

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "init" command with the following command:

```
$ sudo auditctl -l | grep init
```

-a always,exit -F path=/usr/sbin/init -F perm=x -F auid>=1000 -F auid!=unset -k privileged-init

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the audit system generates an audit event for any successful/unsuccessful uses of the "init" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

-a always,exit -F path=/usr/sbin/init -F perm=x -F auid>=1000 -F auid!=unset -k privileged-init

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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

1.106 AZLX-23-002180 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the reboot command.

```
GROUP ID: V-274099
RULE ID: SV-274099r1120285
```

Rationale:

Misuse of the reboot command may cause availability issues for the system.

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "reboot" command with the following command:

```
$ sudo auditctl -l | grep reboot
```

-a always,exit -F path=/usr/sbin/reboot -F perm=x -F auid>=1000 -F auid!=unset -k privileged-reboot

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the audit system generates an audit event for any successful/unsuccessful uses of the "reboot" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

-a always,exit -F path=/usr/sbin/reboot -F perm=x -F auid>=1000 -F auid!=unset -k privileged-reboot

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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

1.107 AZLX-23-002185 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the shutdown command.

```
GROUP ID: V-274100
RULE ID: SV-274100r1120288
```

Rationale:

Misuse of the shutdown command may cause availability issues for the system.

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "shutdown" command with the following command:

```
$ sudo auditctl -l | grep shutdown
```

-a always,exit -F path=/usr/sbin/shutdown -F perm=x -F auid>=1000 -F auid!=unset -k privileged-shutdown

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the audit system generates an audit event for any successful/unsuccessful uses of the "shutdown" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

-a always,exit -F path=/usr/sbin/shutdown -F perm=x -F auid>=1000 -F auid!=unset -k privileged-shutdown

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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

1.108 AZLX-23-002190 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit tools must have a mode of "0755" or less permissive.

```
GROUP ID: V-274101
RULE ID: SV-274101r1120291
```

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.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys 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 Amazon Linux 2023 audit tools have a mode of "0755" or less with the following command:

```
$ 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 tool files have a mode more permissive than "0755", this is a finding.

Remediation:

Configure Amazon Linux 2023 audit tools to have a mode of "0755" by running the following command:

```
$ sudo chmod 0755 [audit_tool]
```

Replace "[audit_tool]" with each audit tool that has a more permissive mode than "0755".

Internal Only - General

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

1.109 AZLX-23-002195 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit tools must be owned by root.

```
GROUP ID: V-274102
RULE ID: SV-274102r1120294
```

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.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys 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 Amazon Linux 2023 audit tools are owned by "root" with 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 audit tools do not have an owner of "root", this is a finding.

Remediation:

Configure Amazon Linux 2023 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".

Internal Only - General

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

1.110 AZLX-23-002200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit tools must be group-owned by root.

```
GROUP ID: V-274103
RULE ID: SV-274103r1120297
```

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.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys 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 Amazon Linux 2023 audit tools are group owned by "root" with the following command:

```
$ 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 audit tools do not have a group owner of "root", this is a finding.

Remediation:

Configure Amazon Linux 2023 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".

Internal Only - General

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

1.111 AZLX-23-002205 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

```
GROUP ID: V-274104
RULE ID: SV-274104r1120300
```

Rationale:

Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221, SRG-OS-000274-GPOS-00104, SRG-OS-000275-GPOS-00105, SRG-OS-000276-GPOS-00106, SRG-OS-000277-GPOS-00107

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/passwd)'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Enable the auditd daemon so that it can start at boot time:

```
$ sudo systemctl enable auditd
```

Add or update the following file system rule to "/etc/audit/rules.d/audit.rules": -w /etc/passwd -p wa -k identity

Then, restart the auditd service 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-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-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-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)

Internal Only - General

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

Internal Only - General

1.112 AZLX-23-002210 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all successful/unsuccessful uses of the chage command.

```
GROUP ID: V-274105
RULE ID: SV-274105r1120661
```

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.

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-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify Amazon Linux 2023 is configured so that an audit event is generated for any successful/unsuccessful use of the "chage" command by performing 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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the audit service generates an audit event for any successful/unsuccessful uses 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

Internal Only - General

- 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

1.113 AZLX-23-002215 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must alert the information system security officer (ISSO) and system administrator (SA), at a minimum, in the event of an audit processing failure.

```
GROUP ID: V-274106
RULE ID: SV-274106r1120657
```

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 Amazon Linux 2023 is configured to notify the SA and ISSO, at a minimum, 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.

Remediation:

Configure Amazon Linux 2023 so that the "auditd" service notifies the SA and ISSO in the event of an audit processing failure.

Edit the following line in "/etc/audit/auditd.conf" to ensure administrators are notified via email for those situations:

action_mail_acct = 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

1.114 AZLX-23-002220 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must off-load audit records onto a different system in the event the audit storage volume is full.

```
GROUP ID: V-274107
RULE ID: SV-274107r1120309
```

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.

Audit:

Verify Amazon Linux 2023 takes the appropriate action when the audit storage volume is full using the following command:

```
$ sudo grep disk_full_action /etc/audit/auditd.conf
```

disk_full_action = SYSLOG

If the value of the "disk_full_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, ask the system administrator to indicate how the system takes appropriate action when an audit storage volume is full. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure Amazon Linux 2023 to off-load audit logs in the event the audit storage volume becomes full.

Add or update the following line (depending on configuration "disk_full_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in "/etc/audit/auditd.conf" file:

disk_full_action = SYSLOG

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

1.115 AZLX-23-002225 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit logs must be group-owned by root or by a restricted logging group to prevent unauthorized read access.

```
GROUP ID: V-274108
RULE ID: SV-274108r1120312
```

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 operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify Amazon Linux 2023 audit logs are group-owned by "root" or a restricted logging group.

First determine if a group other than "root" has been assigned to the audit logs with the following command:

```
$ sudo grep log_group /etc/audit/auditd.conf
```

log_group = root

Then 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

Then using the location of the audit log file, determine if the audit log is group-owned by "root" using the following command:

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

root /var/log/audit/audit.log

If the audit log is not group-owned by "root" or the configured alternative logging group, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that audit logs are group-owned by "root" or a restricted logging group.

Change the group of the directory of "/var/log/audit" to be owned by a correct group.

Identify the group that is configured to own audit log:

```
$ sudo grep -P '^[ ]*log_group[ ]+=.*$' /etc/audit/auditd.conf
```

Change the ownership to that group:

```
$ sudo chgrp ${GROUP} /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

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

1.116 AZLX-23-002230 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit log directory must be owned by root to prevent unauthorized read access.

```
GROUP ID: V-274109
RULE ID: SV-274109r1120315
```

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 operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify Amazon Linux 2023 audit logs directory is owned by "root".

First 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

Then using the location of the audit log file, determine if the audit log directory is owned by "root" using the following command:

```
$ 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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the audit logs directory is protected from unauthorized read access by setting the correct owner as "root" with the following command:

```
$ sudo chown root /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

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

1.117 AZLX-23-002235 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit logs file must have mode "0600" or less permissive to prevent unauthorized access to the audit log.

```
GROUP ID: V-274110
RULE ID: SV-274110r1120318
```

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 operating system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify Amazon Linux 2023 audit logs have a mode of "0600".

First 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

Then using the location of the audit log file, determine if the audit log files as a mode of "0640" with the following command:

```
$ sudo find /var/log/audit/ -type f -exec stat -c '%a %n' {} \;
```

600 /var/log/audit/audit.log

If the audit logs have a mode more permissive than "0600", this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the audit logs have a mode of "0600".

Replace "[audit_log_file]" to the correct audit log path, by default this location is "/var/log/audit/audit.log".

```
$ sudo chmod 0600 /var/log/audit/[audit_log_file]
```

Check the group that owns the system audit logs:

```
$ sudo grep -iw log_group /etc/audit/auditd.conf
```

If the log_group is not defined or it is set to root, configure the permissions as follows:

```
$ sudo chmod 0640 $log_file
$ sudo chmod 0440 $log_file.*
```

Otherwise, configure the permissions as follows:

```
$ sudo chmod 0600 $log_file
$ sudo chmod 0400 $log_file.*
```

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

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

1.118 AZLX-23-002240 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 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-274111
RULE ID: SV-274111r1120321
```

Rationale:

Without the capability to restrict which roles and individuals 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 Amazon Linux 2023 is configured so that files in "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive by using the following commands:

```
$ sudo find /etc/audit/rules.d/ /etc/audit/audit.rules /etc/audit/auditd.conf
-type f -exec stat -c "%a %n" {} \;
```

600 /etc/audit/rules.d/audit.rules 640 /etc/audit/audit.rules 640 /etc/audit/auditd.conf

If the files in the "/etc/audit/rules.d/" directory or the "/etc/audit/auditd.conf" file have a mode more permissive than "0640", this is a finding.

Remediation:

Configure Amazon Linux 2023 so that files in "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive with the following commands:

```
$ sudo chmod 0640 /etc/audit/rules.d/audit.rules
$ sudo chmod 0640 /etc/audit/rules.d/[customrulesfile].rules
$ sudo chmod 0640 /etc/audit/auditd.conf
```


Internal Only - General

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

1.119 AZLX-23-002245 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must audit all uses of the sudo command.

```
GROUP ID: V-274112
RULE ID: SV-274112r1120324
```

Rationale:

Without generating audit records 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-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

Audit:

Verify Amazon Linux 2023 is configured to audit the execution of the "sudo" command with the following command:

```
$ sudo auditctl -l | grep '/usr/bin/sudo\b'
```

-a always,exit -S all -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=-1 -F key=priv_cmd

If the command does not return a line, or the line is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that the audit system generates an audit event for any successful/unsuccessful 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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

1.120 AZLX-23-002250 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

```
GROUP ID: V-274113
RULE ID: SV-274113r1120327
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) (SAs) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221, SRG-OS-000274-GPOS-00104, SRG-OS-000275-GPOS-00105, SRG-OS-000276-GPOS-00106, SRG-OS-000277-GPOS-00107

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/passwd)'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.121 AZLX-23-002255 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

```
GROUP ID: V-274114
RULE ID: SV-274114r1120330
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) (SAs) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, 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-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221, SRG-OS-000275-GPOS-00105

Audit:

Verify Amazon Linux 2023 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow with the following command:

```
$ sudo auditctl -l | egrep '(/etc/shadow)'
```

-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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to generate audit records for all account creations, modifications, disabling, and termination 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

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

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-000015 Support the management of system accounts using organization-defined automated mechanisms.

Internal Only - General

- 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-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-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)

Internal Only - General

1.122 AZLX-23-002260 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must produce audit records containing information to establish the identity of any individual or process associated with the event.

```
GROUP ID: V-274115
RULE ID: SV-274115r1120333
```

Rationale:

Without information that establishes the identity of the subjects (i.e., users or processes acting on behalf of users) associated with the events, security personnel cannot determine responsibility for the potentially harmful event.

Audit:

Verify Amazon Linux 2023 is configured so that the audit system resolves 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 Amazon Linux 2023 so that the audit system resolves audit information before writing to disk.

Edit 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.

Additional Information:

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

Internal Only - General

1.123 AZLX-23-002265 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit logs must be group-owned by root or by a restricted logging group to prevent unauthorized read access.

```
GROUP ID: V-274116
RULE ID: SV-274116r1120336
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the audit logs are group-owned by "root" or a restricted logging group.

First determine if a group other than "root" has been assigned to the audit logs with the following command:

```
$ sudo grep log_group /etc/audit/auditd.conf
```

Then 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

Then using the location of the audit log file, determine if the audit log is group-owned by "root" using the following command:

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

root /var/log/audit/audit.log

If the audit log is not group-owned by "root" or the configured alternative logging group, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to change the group of the directory of "/var/log/audit" to be owned by a correct group.

Identify the group that is configured to own audit log:

```
$ sudo grep -P '^[ ]*log_group[ ]+=.*$' /etc/audit/auditd.conf
```

Change the ownership to that group:

```
$ sudo chgrp ${GROUP} /var/log/audit
```

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

1.124 AZLX-23-002270 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the audit log directory be owned by root to prevent unauthorized read access.

```
GROUP ID: V-274117
RULE ID: SV-274117r1120339
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the audit logs directory is owned by "root".

First 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

Then using the location of the audit log file, determine if the audit log directory is owned by "root" using the following command:

sudo stat -c '%U %n' /var/log/audit root /var/log/audit

If the audit log directory is not owned by "root", this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 audit logs to be protected from unauthorized read access by setting the correct owner as "root" with the following command:

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

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

1.125 AZLX-23-002275 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit logs file must have mode "0600" or less permissive to prevent unauthorized access to the audit log.

```
GROUP ID: V-274118
RULE ID: SV-274118r1120342
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the audit logs have a mode of "0600".

First 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

Then using the location of the audit log file, determine if the audit log files as a mode of "0640" with the following command:

```
$ sudo find /var/log/audit/ -type f -exec stat -c '%a %n' {} \;
```

600 /var/log/audit/audit.log

If the audit logs have a mode more permissive than "0600", this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 audit logs to have a mode of "0600" with the following command:

Replace "[audit_log_file]" to the correct audit log path, by default this location is "/var/log/audit/audit.log".

```
$ sudo chmod 0600 /var/log/audit/[audit_log_file]
```

Check the group that owns the system audit logs:

```
$ sudo grep -m 1 -q ^log_group /etc/audit/auditd.conf
```

If the log_group is not defined or it is set to root, configure the permissions as follows:

```
$ sudo chmod 0640 $log_file
$ sudo chmod 0440 $log_file.*
```

Otherwise, configure the permissions as follows:

```
$ sudo chmod 0600 $log_file
$ sudo chmod 0400 $log_file.*
```

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

1.126 AZLX-23-002280 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 library directories must be group-owned by root or a system account.

```
GROUP ID: V-274119
RULE ID: SV-274119r1120345
```

Rationale:

If Amazon Linux 2023 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 operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 systemwide 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 systemwide shared library directory is returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure Amazon Linux 2023 systemwide 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]
```


Internal Only - General

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

1.127 AZLX-23-002285 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 library directories must have mode "755" or less permissive.

```
GROUP ID: V-274120
RULE ID: SV-274120r1120348
```

Rationale:

If Amazon Linux 2023 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 operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 systemwide shared library directories have mode "755" or less permissive with the following command:

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

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

Remediation:

Configure Amazon Linux 2023 systemwide 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 with a mode more permissive than "755".

```
$ sudo chmod 755 [DIRECTORY]
```


Internal Only - General

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

1.128 AZLX-23-002290 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 library files must have mode "755" or less permissive.

```
GROUP ID: V-274121
RULE ID: SV-274121r1155161
```

Rationale:

If Amazon Linux 2023 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 operating systems 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 Amazon Linux 2023 systemwide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" have mode 0755 or less permissive.

Check that the systemwide shared library files have mode 0755 or less permissive with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -type f -name '*.so*' -perm /022
-exec stat -c "%n %a" {} +
```

If any output is returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 systemwide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" have mode 0755 or less permissive with the following command.

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -type f -name '*.so*' -perm /022
-exec chmod go-w {} +
```


Internal Only - General

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

1.129 AZLX-23-002295 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 library files must be owned by root.

```
GROUP ID: V-274122
RULE ID: SV-274122r1155164
```

Rationale:

If Amazon Linux 2023 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 operating systems 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 shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 systemwide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" are owned by root with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -type f -name '*.so*' ! -user
root -exec stat -c "%n %U" {} +
```

If any output is returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 systemwide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" to be owned by root with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -type f -name '*.so*' ! -user
root -exec chown root {} +
```

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

1.130 AZLX-23-002300 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 library files must be group-owned by root or a system account.

```
GROUP ID: V-274123
RULE ID: SV-274123r1155167
```

Rationale:

If Amazon Linux 2023 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 operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 systemwide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" are group owned by root with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -type f -name '*.so*' ! -group
root -exec stat -c "%n %G" {} +
```

If any output is returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 systemwide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" to be group owned by root with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 -type f -name '*.so*' ! -group
root -exec chown :root {} +
```


Internal Only - General

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

1.131 AZLX-23-002305 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 library directories must be owned by root.

```
GROUP ID: V-274124
RULE ID: SV-274124r1120360
```

Rationale:

If Amazon Linux 2023 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 operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 systemwide 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 systemwide shared library directory is not owned by root, this is a finding.

Remediation:

Configure Amazon Linux 2023 systemwide 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]
```


Internal Only - General

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

1.132 AZLX-23-002315 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the /var/log directory have mode "0755" or less permissive.

```
GROUP ID: V-274125
RULE ID: SV-274125r1120363
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the "/var/log" directory has a mode of "0755" or less permissive with the following command:

```
$ stat -c '%a %n' /var/log
```

755 /var/log

If "/var/log" does not have a mode of "0755" or less permissive, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the "/var/log" directory has a mode of "0755" by running the following command:

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


Internal Only - General

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

1.133 AZLX-23-002320 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the /var/log directory be owned by root.

```
GROUP ID: V-274126
RULE ID: SV-274126r1120366
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the "/var/log" directory is owned by root with the following command:

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

root /var/log

If "/var/log" does not have an owner of "root", this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the directory "/var/log" is owned by "root" with 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

1.134 AZLX-23-002325 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the /var/log directory be group-owned by root.

```
GROUP ID: V-274127
RULE ID: SV-274127r1120369
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so the "/var/log" directory is group-owned by root with the following command:

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

root /var/log

If "/var/log" does not have a group owner of "root", this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the "/var/log" is group-owned "root" with 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

1.135 AZLX-23-002330 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the /var/log/messages file have mode "0640" or less permissive.

```
GROUP ID: V-274128
RULE ID: SV-274128r1120372
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the "/var/log/messages" file has a mode of "0640" or less permissive with the following command:

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

600 /var/log/messages

If "/var/log/messages" does not have a mode of "0640" or less permissive, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the "/var/log/messages" file has a mode of "0640" with the following command:

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


Internal Only - General

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

1.136 AZLX-23-002335 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the /var/log/messages file be group-owned by root.

```
GROUP ID: V-274129
RULE ID: SV-274129r1120375
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the "/var/log/messages" file is group-owned by root with the following command:

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

root /var/log/messages

If "/var/log/messages" does not have a group owner of "root", this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the "/var/log/messages" file is group-owned "root" with 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

1.137 AZLX-23-002340 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the /var/log/messages file be owned by root.

```
GROUP ID: V-274130
RULE ID: SV-274130r1120378
```

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 Amazon Linux 2023 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 Amazon Linux 2023 is configured so that the "/var/log/messages" file is owned by root with the following command:

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

root /var/log/messages

If "/var/log/messages" does not have an owner of "root", this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the "/var/log/messages" file is owned by "root" with 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

1.138 AZLX-23-002345 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 system commands must be owned by root.

```
GROUP ID: V-274131
RULE ID: SV-274131r1120381
```

Rationale:

If Amazon Linux 2023 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 operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 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/libexec /usr/local/bin
/usr/local/sbin ! -user root -exec ls -l {} \;
```

If any system commands are found to not be owned by root, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that system commands are protected from unauthorized access.

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

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


Internal Only - General

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

1.139 AZLX-23-002350 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 system commands must be group-owned by root or a system account.

```
GROUP ID: V-274132
RULE ID: SV-274132r1120384
```

Rationale:

If Amazon Linux 2023 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 operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify Amazon Linux 2023 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 Amazon Linux 2023 so that system commands are 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]
```


Internal Only - General

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

1.140 AZLX-23-002355 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-274133
RULE ID: SV-274133r1120387
```

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.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000725-GPOS-00180

Audit:

Verify Amazon Linux 2023 enforces password complexity by requiring that at least one uppercase character with the following command:

```
$ sudo grep ucredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

ucredit = -1

If the value of "ucredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 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 to contain the "ucredit" parameter:

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-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

Internal Only - General

1.141 AZLX-23-002360 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce password complexity by requiring that at least one lowercase character be used.

```
GROUP ID: V-274134
RULE ID: SV-274134r1120390
```

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.

Satisfies: SRG-OS-000070-GPOS-00038, SRG-OS-000725-GPOS-00180

Audit:

Verify Amazon Linux 2023 enforces password complexity by requiring that at least one lowercase character with the following command:

```
$ sudo grep lcredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

lcredit = -1

If the value of "lcredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 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 to contain the "lcredit" parameter:

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-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

Internal Only - General

1.142 AZLX-23-002365 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-274135
RULE ID: SV-274135r1120393
```

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.

Satisfies: SRG-OS-000071-GPOS-00039, SRG-OS-000725-GPOS-00180

Audit:

Verify Amazon Linux 2023 enforces password complexity by requiring that at least one numeric character with the following command:

```
$ sudo grep dcredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

dcredit = -1

If the value of "dcredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 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 to contain the "dcredit" parameter:

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-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

Internal Only - General

1.143 AZLX-23-002370 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must require the change of at least 50 percent of the total number of characters when passwords are changed.

```
GROUP ID: V-274136
RULE ID: SV-274136r1120697
```

Rationale:

If Amazon Linux 2023 allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least 8 characters.

Satisfies: SRG-OS-000072-GPOS-00040, SRG-OS-000725-GPOS-00180

Audit:

Verify Amazon Linux 2023 enforces password complexity by requiring that at least a change of at least eight characters when passwords are changed with the following command:

```
$ sudo grep difok /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

difok = 8

If the value of "difok" is set to less than "8", or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to require the change of at least eight (with a 15 character password) 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 to contain the "difok" parameter:

difok = 8

Remove any configurations that conflict with the above value. This value can be customized based on desired password length.

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-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

Internal Only - General

1.144 AZLX-23-002375 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce a minimum 15-character password length.

```
GROUP ID: V-274137
RULE ID: SV-274137r1120725
```

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 exponentially increase the time and/or resources required to compromise the password.

Satisfies: SRG-OS-000078-GPOS-00046, SRG-OS-000725-GPOS-00180

Audit:

Verify Amazon Linux 2023 enforces a minimum 15-character password length with the following command:

```
$ sudo grep -rs minlen /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

/etc/security/pwquality.conf: minlen = 15

If the command does not return a "minlen" value of 15 or greater, or the line is commented out, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure Amazon Linux 2023 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 to contain the "minlen" parameter:

minlen = 15

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-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

Internal Only - General

1.145 AZLX-23-002380 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-274138
RULE ID: SV-274138r1120402
```

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 in determining 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.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

Satisfies: SRG-OS-000266-GPOS-00101, SRG-OS-000725-GPOS-00180

Audit:

Verify Amazon Linux 2023 enforces password complexity by requiring at least one special character with the following command:

```
$ sudo grep -rs ocredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

/etc/security/pwquality.conf: ocredit = -1

If the value of "ocredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to enforce password complexity by requiring 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 to contain the "ocredit" parameter:

ocredit = -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-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

Internal Only - General

1.146 AZLX-23-002385 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce password complexity rules for the root account.

```
GROUP ID: V-274139
RULE ID: SV-274139r1120405
```

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.

Satisfies: SRG-OS-000072-GPOS-00040, SRG-OS-000071-GPOS-00039, SRG-OS-000070-GPOS-00038, SRG-OS-000266-GPOS-00101, SRG-OS-000078-GPOS-00046, SRG-OS-000069-GPOS-00037

Audit:

Verify Amazon Linux 2023 enforces password complexity rules for the root account with the following command:

```
$ sudo grep -rs enforce_for_root /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

/etc/security/pwquality.conf:enforce_for_root

If "enforce_for_root" is commented or missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 to enforce password complexity on the root account.

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 to contain the "enforce_for_root" parameter:

enforce_for_root

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)

Internal Only - General

1.147 AZLX-23-002390 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must prevent the use of dictionary words for passwords.

```
GROUP ID: V-274140
RULE ID: SV-274140r1120408
```

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. If Amazon Linux 2023 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.

Satisfies: SRG-OS-000480-GPOS-00225, SRG-OS-000710-GPOS-00160

Audit:

Verify Amazon Linux 2023 prevents the use of dictionary words for passwords with the following command:

```
$ sudo grep -rs dictcheck /etc/security/pwquality.conf
/etc/pwquality.conf.d/*.conf
```

/etc/security/pwquality.conf:dictcheck=1

If the "dictcheck" parameter is not set to "1", is commented out, or is missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 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/pwquality.conf.d/ directory to contain the "dictcheck" parameter:

dictcheck=1

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

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

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

Internal Only - General

1.148 AZLX-23-002395 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

Amazon Linux 2023 must limit the number of concurrent sessions to ten for all accounts and/or account types.

```
GROUP ID: V-274141
RULE ID: SV-274141r1120411
```

Rationale:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to denial-of-service (DoS) 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 Amazon Linux 2023 limits the number of concurrent sessions to "10" for all accounts and/or account types with the following command:

```
$ sudo grep -r -s '^[^#].*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, commented out, or the value is set greater than "10" and is not documented with the information system security officer (ISSO) as an operational requirement for all domains that have the "maxlogins" item assigned, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to limit the number of concurrent sessions to "10" for all accounts and/or account types.

Add the following line to the top of the /etc/security/limits.conf or in a ".conf" file defined in /etc/security/limits.d/:

- hard maxlogins 10

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

1.149 AZLX-23-002396 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically exit interactive command shell user sessions after 15 minutes of inactivity.

```
GROUP ID: V-274142
RULE ID: SV-274142r1120414
```

Rationale:

Terminating an idle interactive command shell user session within a short time period reduces the window of opportunity for unauthorized personnel to take control of it when left unattended in a virtual terminal or physical console.

Audit:

Verify Amazon Linux 2023 is configured to exit interactive command shell user sessions after 10 minutes of inactivity or less with the following command:

```
$ sudo grep -i tmout /etc/profile /etc/profile.d/*.sh
```

/etc/profile.d/tmout.sh:declare -xr TMOUT=600

If "TMOUT" is not set to "600" or less in a script located in the "/etc/'profile.d/ directory, is missing or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to exit interactive command shell user sessions after 10 minutes of inactivity.

Add or edit the following line in "/etc/profile.d/tmout.sh":

#!/bin/bash

declare -xr TMOUT=600

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-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

1.150 AZLX-23-002400 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce 24 hours/1 day as the minimum password lifetime.

```
GROUP ID: V-274143
RULE ID: SV-274143r1120417
```

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, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Verify Amazon Linux 2023 enforces 24 hours as the minimum password lifetime for new user accounts 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 Amazon Linux 2023 to enforce 24 hours as the minimum password lifetime for new user accounts.

Add the following line in "/etc/login.defs" (or modify the line to have the required value):

PASS_MIN_DAYS 1

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)

Internal Only - General

1.151 AZLX-23-002405 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-274144
RULE ID: SV-274144r1120420
```

Rationale:

Increasing the time between a failed authentication attempt and re-prompting to enter credentials helps to slow a single-threaded brute force attack.

Audit:

Verify Amazon Linux 2023 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, the line is commented out, or the line is missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 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

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

1.152 AZLX-23-002410 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

```
GROUP ID: V-274145
RULE ID: SV-274145r1120423
```

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Satisfies: SRG-OS-000480-GPOS-00228, SRG-OS-000480-GPOS-00230

Audit:

Verify Amazon Linux 2023 defines default permissions for all authenticated users in such a way that the user can only read and modify their own files with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in "/etc/login.defs" file, the Severity is raised to a CAT I.

grep -i umask /etc/login.defs

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.

Remediation:

Configure Amazon Linux 2023 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/login.defs" file to "077":

UMASK 077

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

1.153 AZLX-23-002415 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically remove or disable temporary user accounts after 72 hours.

```
GROUP ID: V-274146
RULE ID: SV-274146r1120426
```

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.

Audit:

Verify Amazon Linux 2023 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.

Remediation:

Configure Amazon Linux 2023 temporary accounts to have an expiration date of 72 hours.

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 +3days +%Y-%m-%d) system_account_name
```


Internal Only - General

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

1.154 AZLX-23-002420 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically lock an account when three unsuccessful logon attempts occur.

```
GROUP ID: V-274147
RULE ID: SV-274147r1120429
```

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.

Amazon Linux 2023 can utilize 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 re-enabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

Audit:

Verify Amazon Linux 2023 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 met by that method.

```
$ 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, if any of the lines are commented out, or are missing, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to lock an account when three 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
```

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

Internal Only - General

1.155 AZLX-23-002425 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must be able to enforce a 60-day maximum password lifetime restriction.

```
GROUP ID: V-274148
RULE ID: SV-274148r1120432
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If Amazon Linux 2023 does not limit the lifetime of passwords and force users to change their passwords, there is the risk that Amazon Linux 2023 passwords could be compromised.

Audit:

Verify Amazon Linux 2023 enforces 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 Amazon Linux 2023 to set noncompliant 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)

Internal Only - General

1.156 AZLX-23-002430 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

```
GROUP ID: V-274149
RULE ID: SV-274149r1120435
```

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.

Operating systems need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Satisfies: SRG-OS-000118-GPOS-00060, SRG-OS-000590-GPOS-00110

Audit:

Verify Amazon Linux 2023 account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity with the following command:

Check the account inactivity value by performing the following command:

```
$ sudo grep -i inactive /etc/default/useradd
```

INACTIVE=35

If "INACTIVE" is set to "-1", a value greater than "35", or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to disable account identifiers after 35 days of inactivity after the password expiration.

Run the following command to change the configuration for useradd:

```
$ sudo useradd -D -f 35
```

The recommendation is 35 days, but a lower value is acceptable.

Internal Only - General

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)

Internal Only - General

1.157 AZLX-23-002435 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically expire temporary accounts within 72 hours.

```
GROUP ID: V-274150
RULE ID: SV-274150r1120438
```

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 exploitation 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 must be established for privileged users who need long-term maintenance accounts.

Audit:

Verify Amazon Linux 2023 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 Amazon Linux 2023 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

1.158 AZLX-23-002440 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must restrict the use of the "su" command.

```
GROUP ID: V-274151
RULE ID: SV-274151r1120441
```

Rationale:

The "su" program allows to run commands with a substitute user and group ID. It is commonly used to run commands as the root user. Limiting access to such commands is considered a good security practice.

Audit:

Verify Amazon Linux 2023 requires uses to be members of the "wheel" group with the following command:

```
$ grep pam_wheel /etc/pam.d/su
```

auth required pam_wheel.so use_uid

If a line for "pam_wheel.so" does not exist, or is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to require users to be in the "wheel" group to run "su" command.

In file "/etc/pam.d/su", uncomment the following line:

```
"#auth required pam_wheel.so use_uid"
$ sudo sed
'/^[[:space:]]*#[[:space:]]*auth[[:space:]]\+required[[:space:]]\+pam_wheel\.
so[[:space:]]\+use_uid$/s/^[[:space:]]*#//' -i /etc/pam.d/su
```

If necessary, create a "wheel" group and add administrative users to the group.

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

1.159 AZLX-23-002445 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enable the SELinux targeted policy.

```
GROUP ID: V-274152
RULE ID: SV-274152r1120738
```

Rationale:

Setting the SELinux policy to "targeted" or a more specialized policy ensures the system will confine processes that are likely to be targeted for exploitation, such as network or system services.

Note: During the development or debugging of SELinux modules, it is common to temporarily place nonproduction systems in "permissive" mode. In such temporary cases, SELinux policies should be developed, and once work is completed, the system should be reconfigured to "targeted".

Audit:

Verify Amazon Linux 2023 SELINUX is using the targeted policy with the following command:

```
$ sestatus | grep policy
```

Loaded policy name: targeted

If the loaded policy name is not "targeted", this is a finding.

Remediation:

Configure Amazon Linux 2023 to use the targeted SELINUX policy.

Edit the file "/etc/selinux/config" and add or modify 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

1.160 AZLX-23-002450 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

Amazon Linux 2023 must use a Linux Security Module configured to enforce limits on system services.

```
GROUP ID: V-274153
RULE ID: SV-274153r1120713
```

Rationale:

An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are 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. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For nonkernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries. Operating systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000445-GPOS-00199

Audit:

Verify Amazon Linux 2023 verifies the correct operation of security functions through the use of SELinux with the following command:

```
$ getenforce
```

Enforcing

If SELINUX is not set to "Enforcing", this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to verify correct operation of security functions.

Edit the file "/etc/selinux/config" and add or modify the following line:

SELINUX=enforcing

A reboot is required for the changes to take effect.

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

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

1.161 AZLX-23-002455 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically lock an account when three unsuccessful logon attempts occur.

```
GROUP ID: V-274154
RULE ID: SV-274154r1120450
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Audit:

Verify Amazon Linux 2023 is configured to lock an account after three unsuccessful logon attempts with the command:

```
$ grep 'deny =' /etc/security/faillock.conf
```

deny = 3

If the "deny" option is not set to "3" or less (but not "0"), is missing or commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 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-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

1.162 AZLX-23-002460 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically lock the root account until the root account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-274155
RULE ID: SV-274155r1120453
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Audit:

Verify Amazon Linux 2023 is configured to lock the root account after three unsuccessful logon attempts with the command:

```
$ grep even_deny_root /etc/security/faillock.conf
```

even_deny_root

If the "even_deny_root" option is not set, is missing or commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to lock out the "root" account after a number of incorrect login attempts using "pam_faillock.so", first enable the feature using the following command:

```
$ sudo authselect enable-feature with-faillock
```

Then edit the "/etc/security/faillock.conf" file as follows:

add or uncomment the following line: even_deny_root

Additional Information:

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

1.163 AZLX-23-002465 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes occur.

```
GROUP ID: V-274156
RULE ID: SV-274156r1120456
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Audit:

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.

Verify Amazon Linux 2023 locks an account after three unsuccessful logon attempts within a period of 15 minutes with the following command:

```
$ grep fail_interval /etc/security/faillock.conf
```

fail_interval = 900

If the "fail_interval" option is not set to "900" or less (but not "0"), the line is commented out, or the line is missing, this is a finding.

Remediation:

Configure Amazon Linux 2023 to automatically lock an account after three unsuccessful logon attempts in 15-minutes.

First, ensure that the system is configured with authselect, i.e., using sssd profiles:

```
$ sudo authselect select sssd [--force]
```

Then, enable the faillock feature:

```
$ sudo authselect enable-feature with-faillock
```

Then edit the "/etc/security/faillock.conf" file as follows:

fail_interval = 900

Internal Only - General

Additional Information:

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

1.164 AZLX-23-002470 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must maintain an account lock until the locked account is released by an administrator.

```
GROUP ID: V-274157
RULE ID: SV-274157r1120459
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Audit:

Verify Amazon Linux 2023 is configured to lock an account until released by an administrator after three unsuccessful logon attempts with the command:

```
$ grep 'unlock_time =' /etc/security/faillock.conf
```

unlock_time = 0

If the "unlock_time" option is not set to "0", the line is missing, or commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 to lock an account until released by an administrator after three unsuccessful logon attempts with the command:

```
$ authselect enable-feature with-faillock
```

Then edit the "/etc/security/faillock.conf" file as follows:

unlock_time = 0

Additional Information:

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

1.165 AZLX-23-002475 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 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 Category Assurance List (PPSM CAL) and vulnerability assessments.

```
GROUP ID: V-274158
RULE ID: SV-274158r1120727
```

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 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, Amazon Linux 2023 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.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Audit:

Verify Amazon Linux 2023 firewall is configured to block unregistered ports, protocols, and services.

Inspect the list of enabled firewall ports and verify they are configured correctly by running the following command:

```
$ sudo firewall-cmd --list-all
```

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, or there are no firewall rules configured, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to Prohibit/Restrict Functions, Ports, Protocols, Services. Use firewall-cmd to manage firewalld.

For example, to block a specific port (8080), use: sudo firewall-cmd --permanent --remove-port=8080/tcp

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

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

1.166 AZLX-23-002480 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must insure all interactive users have a primary group that exists.

```
GROUP ID: V-274159
RULE ID: SV-274159r1120465
```

Rationale:

If a user is assigned the group identifier (GID) of a group that does not exist on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000121-GPOS-00062, SRG-OS-000042-GPOS-00020

Audit:

Verify Amazon Linux 2023 interactive users have a valid GID with the following command:

```
$ sudo pwck -qr
```

If the system has any interactive users with duplicate GIDs, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that all GIDs are referenced in "/etc/passwd" are defined in "/etc/group".

Edit the file "/etc/passwd" and ensure that every user's GID is a valid GID.

Internal Only - General

Additional Information:

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

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

1.167 AZLX-23-002485 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure all interactive users have unique User IDs (UIDs).

```
GROUP ID: V-274160
RULE ID: SV-274160r1120663
```

Rationale:

To ensure accountability and prevent unauthenticated access, interactive users must be identified and authenticated to prevent potential misuse and compromise of the system.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000121-GPOS-00062, SRG-OS-000042-GPOS-00020

Audit:

Verify Amazon Linux 2023 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:

Configure Amazon Linux 2023 to contain no duplicate UIDs for interactive users.

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-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

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

1.168 AZLX-23-002489 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the password complexity module is enabled in the password-auth file.

```
GROUP ID: V-274161
RULE ID: SV-274161r1120471
```

Rationale:

Enabling PAM password complexity permits enforcement of strong passwords and consequently makes the system less prone to dictionary attacks.

Audit:

Verify Amazon Linux 2023 uses "pwquality" to enforce the password complexity rules in the password-auth file with the following command:

```
$ grep pam_pwquality /etc/pam.d/password-auth
```

password required pam_pwquality.so

If the command does not return a line containing the value "pam_pwquality.so", or the line is commented out, this is a finding.

If the system administrator can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

Configure Amazon Linux 2023 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 required pam_pwquality.so

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

1.169 AZLX-23-002490 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 password-auth must be configured to use a sufficient number of hashing rounds.

```
GROUP ID: V-274162
RULE ID: SV-274162r1120474
```

Rationale:

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

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

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

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify Amazon Linux 2023 has the required number of rounds for the password hashing algorithm is configured in password-auth with the following command:

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

password sufficient pam_unix.so sha512 rounds=100000

If a matching line is not returned or "rounds" is less than "100000", this a finding.

Remediation:

Configure Amazon Linux 2023 to use 100000 hashing rounds for hashing passwords.

Add or modify the following line in "/etc/pam.d/password-auth" and set "rounds" to "100000".

password sufficient pam_unix.so sha512 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-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

1.170 AZLX-23-002495 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 system-auth must be configured to use a sufficient number of hashing rounds.

```
GROUP ID: V-274163
RULE ID: SV-274163r1120477
```

Rationale:

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

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

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

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify Amazon Linux 2023 has the required number of rounds for the password hashing algorithm is configured in system-auth with the following command:

```
$ sudo grep rounds /etc/pam.d/system-auth
```

password sufficient pam_unix.so sha512 rounds=100000

If a matching line is not returned or "rounds" is less than "100000", this a finding.

Remediation:

Configure Amazon Linux 2023 to use 100000 hashing rounds for hashing passwords.

Add or modify the following line in "/etc/pam.d/system-auth" and set "rounds" to "100000".

password sufficient pam_unix.so sha512 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-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

1.171 AZLX-23-002500 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure a sticky bit be set on all public directories.

```
GROUP ID: V-274164
RULE ID: SV-274164r1137695
```

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 Amazon Linux 2023 world-writable directories have the sticky bit set.

Determine if all world-writable directories have the sticky bit set by running the following command:

```
$ sudo find / -type d -perm -0002 ! -perm -1000 -exec ls -ld {} +
```

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

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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 following command:

```
$ sudo find / -type d -perm -0002 ! -perm -1000 -exec chmod +t {} +
```

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

1.172 AZLX-23-002505 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure all world-writable directories be owned by root, sys, bin, or an application user.

```
GROUP ID: V-274165
RULE ID: SV-274165r1137695
```

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 Amazon Linux 2023 world writable directories are owned by root, a system account, or an application account with the following command:

```
$ sudo find / -xdev -type d -perm -0002 ! -user root ! -uid +999 -exec ls -ld
{} +
```

If there is output, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 public directories to be owned by root or a system account to prevent unauthorized and unintended information transferred via shared system resources.

Set the owner of all public directories as root or a system account using the following command:

```
$ sudo find / -xdev -type d -perm -0002 ! -user root ! -uid +999 -exec chown root:root {} +
```

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

1.173 AZLX-23-002510 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must terminate idle user sessions.

```
GROUP ID: V-274166
RULE ID: SV-274166r1155170
```

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. In addition, quickly terminating an idle 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 Amazon Linux 2023 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 Amazon Linux 2023 terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

Verify Amazon Linux 2023 logs out sessions that are idle for 10 minutes with the following command:

```
$ sudo grep -i ^StopIdleSessionSec /etc/systemd/logind.conf
```

StopIdleSessionSec=600

If "StopIdleSessionSec" is not configured to "600" seconds, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to log out idle sessions by editing the /etc/systemd/logind.conf file with the following line:

StopIdleSessionSec=600

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

1.174 AZLX-23-002515 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enable auditing of processes that start prior to the audit daemon.

```
GROUP ID: V-274167
RULE ID: SV-274167r1120489
```

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.

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, SRG-OS-000254-GPOS-00095

Audit:

Verify Amazon Linux 2023 is configured so that GRUB 2 enables auditing of processes that start prior to the audit daemon with the following commands:

Check that the current GRUB 2 configuration enables auditing:

```
$ sudo grubby --info=ALL | grep args | grep -v 'audit=1'
```

If any output is returned, this is a finding.

Check that auditing is enabled by default to persist in kernel updates:

```
$ grep audit /etc/default/grub
```

GRUB_CMDLINE_LINUX="audit=1"

If "audit" is not set to "1", is missing, or is commented out, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 so that GRUB 2 enables auditing of 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)

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-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-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

Internal Only - General

- 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)

Internal Only - General

1.175 AZLX-23-002520 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must allocate an audit_backlog_limit of sufficient size to capture processes that start prior to the audit daemon.

```
GROUP ID: V-274168
RULE ID: SV-274168r1120492
```

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-000254-GPOS-00095, SRG-OS-000341-GPOS-00132

Audit:

Verify Amazon Linux 2023 allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon with the following command:

```
$ sudo grubby --info=ALL | grep args | grep -v 'audit_backlog_limit=8192'
```

If the command returns any outputs, and audit_backlog_limit is less than "8192", this is a finding.

Remediation:

Configure Amazon Linux 2023 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
```


Internal Only - General

Additional Information:

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-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

1.176 AZLX-23-002535 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enable discretionary access control on hardlinks.

```
GROUP ID: V-274169
RULE ID: SV-274169r1120495
```

Rationale:

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 mitigates vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Satisfies: SRG-OS-000312-GPOS-00123, SRG-OS-000324-GPOS-00125

Audit:

Verify Amazon Linux 2023 is configured to enable DAC on hardlinks.

Check the status of the fs.protected_hardlinks kernel parameter with the following command:

```
$ 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.

Remediation:

Configure Amazon Linux 2023 to enable DAC on hardlinks with the following:

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

fs.protected_hardlinks = 1

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```


Internal Only - General

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)

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

1.177 AZLX-23-002540 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must enable kernel parameters to enforce discretionary access control on symlinks.

```
GROUP ID: V-274170
RULE ID: SV-274170r1120498
```

Rationale:

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 user identifier (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().

Satisfies: SRG-OS-000312-GPOS-00123, SRG-OS-000324-GPOS-00125

Audit:

Verify Amazon Linux 2023 is configured to enable DAC on symlinks.

Check the status of the fs.protected_symlinks kernel parameter with the following command:

```
$ 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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 to enable DAC on symlinks with the following:

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

fs.protected_symlinks = 1

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)

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

1.178 AZLX-23-002555 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 debug-shell systemd service must be disabled.

```
GROUP ID: V-274173
RULE ID: SV-274173r1120507
```

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 an additional layer of assurance that it will not be enabled via a dependency in systemd. 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 Amazon Linux 2023 is configured to mask the debug-shell systemd service with the following command:

```
$ sudo systemctl status debug-shell.service
```

O 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 Amazon Linux 2023 to mask the debug-shell systemd service with the following command:

```
$ sudo systemctl disable --now debug-shell.service
$ sudo systemctl mask --now debug-shell.service
```

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

1.179 AZLX-23-002560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 chrony must be configured with a maximum interval of 24 hours between requests sent to a USNO server or a time server designated for the appropriate DOD network.

```
GROUP ID: V-274174
RULE ID: SV-274174r1120510
```

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.

Audit:

Verify Amazon Linux 2023 chrony service specifies a maximum interval of 24 hours between requests sent to a USNO server with the following command:

Note: <USNO/DOD Server> is used in place of a time source IP address.

```
$ sudo grep maxpoll /etc/chrony.conf
```

server <USNO/DOD Server> iburst maxpoll 16

If the "maxpoll" option is not configured, commented out, or set to a number greater than 16 or the line is commented out then this is a finding.

Verify Amazon Linux 2023 chrony service is configured to use authoritative USNO or appropriate DOD time source with the following command:

```
$ sudo grep -i server /etc/chrony.conf
```

server <USNO/DOD Server>

If the parameter "server" is not set, or is not set to an authoritative USNO/DOD time source, then this is a finding.

Remediation:

Configure Amazon Linux 2023 to compare internal information system clocks at least every 24 hours with an NTP server. Ensure the following line is added or updated in /etc/chrony.conf:

server DOD.ntp.server iburst maxpoll 16

Internal Only - General

Additional Information:

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)

Internal Only - General

1.180 AZLX-23-002565 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must synchronize internal information system clocks to the authoritative time source at least every 24 hours.

```
GROUP ID: V-274175
RULE ID: SV-274175r1120659
```

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.

Depending on the infrastructure being used the "pool" directive may not be supported.

Satisfies: SRG-OS-000356-GPOS-00144, SRG-OS-000785-GPOS-00250, SRG-OS-000359-GPOS-00146

Audit:

Verify Amazon Linux 2023 is securely comparing internal information system clocks at least every 24 hours with an NTP server with the following commands:

```
$ sudo grep maxpoll /etc/chrony.conf
```

server 0.us.pool.ntp.mil 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.

Verify the "chrony.conf" file is configured to an authoritative DOD time source by running the following command:

```
$ sudo grep -i server /etc/chrony.conf
```

server 0.us.pool.ntp.mil

If the parameter "server" is not set, or is not set to an authoritative DOD time source, this is a finding.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 chrony service to securely 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-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-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

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

Internal Only - General

1.181 AZLX-23-002570 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must routinely check the baseline configuration for unauthorized changes and notify the system administrator when anomalies in the operation of any security functions are discovered.

```
GROUP ID: V-274176
RULE ID: SV-274176r1120655
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to Amazon Linux 2023. 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 Amazon Linux 2023. Amazon Linux 2023's information management officer (IMO)/information system security officer (ISSO) and system administrators (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.

Internal Only - General

Audit:

Verify Amazon Linux 2023 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:

```
$ sudo ls -al /etc/cron.* | grep aide
```

-rwxr-xr-x 1 root root 29 Nov 22 2015 aide

```
$ grep aide /etc/crontab /var/spool/cron/root
```

/etc/crontab: 30 04 * * * root usr/sbin/aide /var/spool/cron/root: 30 04 * * * root usr/sbin/aide

```
$ sudo more /etc/cron.daily/aide
```

#!/bin/bash /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily aide integrity check run" root@sysname.mil

If the file integrity application does not exist, or 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.

Remediation:

Configure Amazon Linux 2023 so that the file integrity tool runs automatically on the system at least weekly and notifies 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 email at the completion of the analysis.

```
$ sudo more /etc/cron.daily/aide
```

#!/bin/bash /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily aide integrity check run" root@sysname.mil

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

1.182 AZLX-23-002575 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must prevent the loading of a new kernel for later execution.

```
GROUP ID: V-274177
RULE ID: SV-274177r1120519
```

Rationale:

Changes to any software components can have significant effects on the overall security of Amazon Linux 2023. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify Amazon Linux 2023 is configured to disable kernel image loading.

Check the status of the kernel.kexec_load_disabled kernel parameter with the following command:

```
$ 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.

Internal Only - General

Remediation:

Configure Amazon Linux 2023 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

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

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

Internal Only - General

1.183 AZLX-23-002580 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must prevent files with the setuid and setgid bit set from being executed on the /boot/efi directory.

```
GROUP ID: V-274178
RULE ID: SV-274178r1120522
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify Amazon Linux 2023 is configured so that the /boot/efi directory is mounted with the "nosuid" option with the following command:

```
$ mount | grep '\s/boot/efi\s'
```

/dev/sda1 on /boot/efi type vfat (rw,nosuid,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=ascii,shortname=winnt,errors=remount-ro)

If the /boot/efi file system does not have the "nosuid" option set, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the /boot/efi directory is mounted with the "nosuid" option.

Modify "/etc/fstab" to use the "nosuid" option on the "/boot/efi" directory.

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

1.184 AZLX-23-002590 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must mount /dev/shm with the nosuid option.

```
GROUP ID: V-274180
RULE ID: SV-274180r1120528
```

Rationale:

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify Amazon Linux 2023 is configured so that "/dev/shm" is mounted with the "nosuid" option with the following command:

```
$ mount | grep /dev/shm
```

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)

If the /dev/shm file system is mounted without the "noexec" option, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that "/dev/shm" is mounted with the "nosuid" option.

Modify "/etc/fstab" to use the "nosuid" option on the "/dev/shm" file system.

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

1.185 AZLX-23-002585 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must mount /dev/shm with the nodev option.

```
GROUP ID: V-274179
RULE ID: SV-274179r1120525
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify Amazon Linux 2023 is configured so that "/dev/shm" is mounted with the "nodev" option with the following command:

```
$ mount | grep /dev/shm
```

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)

If the /dev/shm file system is mounted without the "nodev" option, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that "/dev/shm" is mounted with the "nodev" option.

Modify "/etc/fstab" to use the "nodev" option on the "/dev/shm" file system.

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

1.186 AZLX-23-002595 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must ensure the pcscd service is active.

```
GROUP ID: V-274181
RULE ID: SV-274181r1120531
```

Rationale:

The information system ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

The daemon program for pcsc-lite and the MuscleCard framework is pcscd. It is a resource manager that coordinates communications with smart card readers and smart cards and cryptographic tokens connected to the system.

Audit:

Verify Amazon Linux 2023 is configured so that the "pcscd" service is active with the following command:

```
$ systemctl is-active pcscd
```

active

If the pcscdservice is not active, this is a finding.

Remediation:

Configure Amazon Linux 2023 so that the "pcscd" service is active with the following command:

```
$ sudo systemctl enable --now pcscd
```

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)

Internal Only - General

1.187 AZLX-23-002600 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 file system automount function must be disabled unless required.

```
GROUP ID: V-274182
RULE ID: SV-274182r1120729
```

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.

Audit:

Verify Amazon Linux 2023 disables the file system automount function with the following command:

```
$ sudo systemctl is-enabled autofs
```

masked

If the returned value is not "masked", "disabled", "Failed to get unit file state for autofs.service for autofs", or "enabled", and is not documented as operational requirement with the information system security officer (ISSO), this is a finding.

Remediation:

Configure Amazon Linux 2023 to disable the ability to automount devices.

The autofs service can be disabled with the following command:

```
$ sudo systemctl mask --now autofs.service
```

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

1.188 AZLX-23-002605 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must protect against or limit the effects of denial-of-service (DoS) attacks by ensuring rate-limiting measures are configured on impacted network interfaces.

```
GROUP ID: V-274183
RULE ID: SV-274183r1120714
```

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 Amazon Linux 2023 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 exist 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.

Audit:

Verify Amazon Linux 2023 is implementing rate-limiting measures on network interfaces to protect against DoS attacks.

Access the AWS Management Console:

Sign in to the AWS Management Console and navigate to the EC2 service.

To locate the Application Load Balancer (ALB) in the EC2 dashboard, go to the "Load Balancers" section and find the ALB.

Check the ALB configuration: Click on the ALB to view its details. The listener configuration for the ALB is located in the "Listener" tab.

Look for the rate limiting settings: Scroll down to the "Rules" section. If rate limiting is enabled, a rule with the "Rate Limit" action will be displayed.

Remediation:

Configure Amazon Linux 2023 to use the AWS ALB rate limiting feature using its built-in rate limiting capabilities. This allows the user to set rate limits at the ALB level, which will apply to all traffic passing through the load balancer.

Internal Only - General

Additional Information:

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

1.189 AZLX-23-002610 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must implement nonexecutable data to protect its memory from unauthorized code execution.

```
GROUP ID: V-274184
RULE ID: SV-274184r1120540
```

Rationale:

The no-execute (NX) feature uses the segmentation feature on all x86 systems to prevent execution in memory higher than a certain address. It writes an address as a limit in the code segment descriptor, to control where code can be executed, on a per-process basis. When the kernel places a process's memory regions such as the stack and heap higher than this address, the hardware prevents execution in that address range. This is enabled by default on the latest Red Hat and Fedora systems if supported by the hardware.

Audit:

Verify Amazon Linux 2023 NX support is enabled with the following command:

```
$ sudo dmesg | grep '[NX|DX]*protection'
```

[0.000000] NX (Execute Disable) protection: active

If "dmesg" does not show "NX (Execute Disable) protection" active, this is a finding.

Remediation:

Configure Amazon Linux 2023 NX support to be enabled by opening a support case via the AWS Console to investigate why NX support is not detected.

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

1.190 AZLX-23-002615 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must remove all software components after updated versions have been installed.

```
GROUP ID: V-274185
RULE ID: SV-274185r1120543
```

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by some adversaries.

Audit:

Verify Amazon Linux 2023 removes all software components after updated versions have been installed with the following command:

```
$ grep clean /etc/dnf/dnf.conf
```

clean_requirements_on_remove=1

If "clean_requirements_on_remove" is not set to "1", "True", or "yes", this is a finding.

Remediation:

Configure Amazon Linux 2023 to remove all software components after updated versions have been installed.

Set the "clean_requirements_on_remove" option to "1" in the "/etc/dnf/dnf.conf" file:

clean_requirements_on_remove=1

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

1.191 AZLX-23-002620 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 must configure the use of the pam_faillock.so module in the /etc/pam.d/system-auth file.

```
GROUP ID: V-274186
RULE ID: SV-274186r1120546
```

Rationale:

If the pam_faillock.so module is not loaded, the system will not correctly lockout accounts to prevent password guessing attacks.

Audit:

Verify Amazon Linux 2023 is configured so that the pam_faillock.so module is present in the "/etc/pam.d/system-auth" file:

```
$ 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.

Remediation:

Configure Amazon Linux 2023 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

Internal Only - General

1.192 AZLX-23-005000 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Amazon Linux 2023 audit system must protect logon user identifiers (UIDs) from unauthorized change.

```
GROUP ID: V-274187
RULE ID: SV-274187r1120715
```

Rationale:

If modification of login UIDs is not prevented, they can be changed by nonprivileged users and make auditing complicated or impossible.

Satisfies: SRG-OS-000462-GPOS-00206, SRG-OS-000475-GPOS-00220, SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify Amazon Linux 2023 is configured so that the audit system prevents unauthorized changes to login UIDs with the following command:

```
$ sudo grep -i immutable /etc/audit/audit.rules
```

--loginuid-immutable

If the "--loginuid-immutable" option is not returned in the "/etc/audit/audit.rules", or the line is commented out, this is a finding.

Remediation:

Configure Amazon Linux 2023 auditing to prevent modification of login UIDs once they are set by adding the following line to /etc/audit/rules.d/audit.rules:

--loginuid-immutable

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```


Internal Only - General

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

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	AZLX-23-000100 (Manual)	☐	☐
1.2	AZLX-23-000110 (Manual)	☐	☐
1.3	AZLX-23-000115 (Automated)	☐	☐
1.4	AZLX-23-000120 (Automated)	☐	☐
1.5	AZLX-23-000125 (Automated)	☐	☐
1.6	AZLX-23-000130 (Manual)	☐	☐
1.7	AZLX-23-000135 (Automated)	☐	☐
1.8	AZLX-23-000200 (Automated)	☐	☐
1.9	AZLX-23-000205 (Automated)	☐	☐
1.10	AZLX-23-000210 (Automated)	☐	☐
1.11	AZLX-23-000215 (Automated)	☐	☐
1.12	AZLX-23-000220 (Automated)	☐	☐
1.13	AZLX-23-000225 (Automated)	☐	☐
1.14	AZLX-23-000300 (Automated)	☐	☐
1.15	AZLX-23-000305 (Automated)	☐	☐
1.16	AZLX-23-000310 (Automated)	☐	☐
1.17	AZLX-23-000315 (Automated)	☐	☐
1.18	AZLX-23-000320 (Automated)	☐	☐
1.19	AZLX-23-001000 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	AZLX-23-001005 (Automated)	☐	☐
1.21	AZLX-23-001010 (Automated)	☐	☐
1.22	AZLX-23-001015 (Automated)	☐	☐
1.23	AZLX-23-001020 (Automated)	☐	☐
1.24	AZLX-23-001025 (Automated)	☐	☐
1.25	AZLX-23-001030 (Automated)	☐	☐
1.26	AZLX-23-001035 (Automated)	☐	☐
1.27	AZLX-23-001040 (Automated)	☐	☐
1.28	AZLX-23-001045 (Automated)	☐	☐
1.29	AZLX-23-001050 (Automated)	☐	☐
1.30	AZLX-23-001055 (Automated)	☐	☐
1.31	AZLX-23-001060 (Automated)	☐	☐
1.32	AZLX-23-001065 (Automated)	☐	☐
1.33	AZLX-23-001070 (Automated)	☐	☐
1.34	AZLX-23-001075 (Automated)	☐	☐
1.35	AZLX-23-001080 (Automated)	☐	☐
1.36	AZLX-23-001085 (Manual)	☐	☐
1.37	AZLX-23-001090 (Automated)	☐	☐
1.38	AZLX-23-001095 (Automated)	☐	☐
1.39	AZLX-23-001105 (Automated)	☐	☐
1.40	AZLX-23-001110 (Automated)	☐	☐
1.41	AZLX-23-001115 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	AZLX-23-001120 (Automated)	☐	☐
1.43	AZLX-23-001125 (Automated)	☐	☐
1.44	AZLX-23-001130 (Automated)	☐	☐
1.45	AZLX-23-001180 (Automated)	☐	☐
1.46	AZLX-23-001185 (Automated)	☐	☐
1.47	AZLX-23-001195 (Automated)	☐	☐
1.48	AZLX-23-001200 (Automated)	☐	☐
1.49	AZLX-23-001205 (Automated)	☐	☐
1.50	AZLX-23-001210 (Automated)	☐	☐
1.51	AZLX-23-001215 (Automated)	☐	☐
1.52	AZLX-23-001220 (Automated)	☐	☐
1.53	AZLX-23-001225 (Automated)	☐	☐
1.54	AZLX-23-001230 (Automated)	☐	☐
1.55	AZLX-23-001235 (Automated)	☐	☐
1.56	AZLX-23-001240 (Automated)	☐	☐
1.57	AZLX-23-001245 (Automated)	☐	☐
1.58	AZLX-23-001250 (Automated)	☐	☐
1.59	AZLX-23-001255 (Automated)	☐	☐
1.60	AZLX-23-001260 (Automated)	☐	☐
1.61	AZLX-23-001265 (Automated)	☐	☐
1.62	AZLX-23-001270 (Automated)	☐	☐
1.63	AZLX-23-001275 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	AZLX-23-001280 (Automated)	☐	☐
1.65	AZLX-23-001285 (Automated)	☐	☐
1.66	AZLX-23-001290 (Automated)	☐	☐
1.67	AZLX-23-001295 (Manual)	☐	☐
1.68	AZLX-23-001300 (Automated)	☐	☐
1.69	AZLX-23-001305 (Automated)	☐	☐
1.70	AZLX-23-001310 (Manual)	☐	☐
1.71	AZLX-23-001315 (Manual)	☐	☐
1.72	AZLX-23-002000 (Manual)	☐	☐
1.73	AZLX-23-002005 (Automated)	☐	☐
1.74	AZLX-23-002015 (Manual)	☐	☐
1.75	AZLX-23-002020 (Automated)	☐	☐
1.76	AZLX-23-002025 (Automated)	☐	☐
1.77	AZLX-23-002030 (Automated)	☐	☐
1.78	AZLX-23-002035 (Automated)	☐	☐
1.79	AZLX-23-002040 (Automated)	☐	☐
1.80	AZLX-23-002045 (Automated)	☐	☐
1.81	AZLX-23-002050 (Automated)	☐	☐
1.82	AZLX-23-002055 (Automated)	☐	☐
1.83	AZLX-23-002060 (Automated)	☐	☐
1.84	AZLX-23-002065 (Automated)	☐	☐
1.85	AZLX-23-002070 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	AZLX-23-002075 (Automated)	☐	☐
1.87	AZLX-23-002080 (Manual)	☐	☐
1.88	AZLX-23-002085 (Automated)	☐	☐
1.89	AZLX-23-002090 (Automated)	☐	☐
1.90	AZLX-23-002095 (Automated)	☐	☐
1.91	AZLX-23-002100 (Automated)	☐	☐
1.92	AZLX-23-002105 (Automated)	☐	☐
1.93	AZLX-23-002110 (Automated)	☐	☐
1.94	AZLX-23-002115 (Automated)	☐	☐
1.95	AZLX-23-002120 (Automated)	☐	☐
1.96	AZLX-23-002125 (Automated)	☐	☐
1.97	AZLX-23-002130 (Automated)	☐	☐
1.98	AZLX-23-002135 (Automated)	☐	☐
1.99	AZLX-23-002140 (Automated)	☐	☐
1.100	AZLX-23-002145 (Automated)	☐	☐
1.101	AZLX-23-002150 (Automated)	☐	☐
1.102	AZLX-23-002155 (Automated)	☐	☐
1.103	AZLX-23-002160 (Automated)	☐	☐
1.104	AZLX-23-002165 (Automated)	☐	☐
1.105	AZLX-23-002175 (Automated)	☐	☐
1.106	AZLX-23-002180 (Automated)	☐	☐
1.107	AZLX-23-002185 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	AZLX-23-002190 (Automated)	☐	☐
1.109	AZLX-23-002195 (Automated)	☐	☐
1.110	AZLX-23-002200 (Automated)	☐	☐
1.111	AZLX-23-002205 (Automated)	☐	☐
1.112	AZLX-23-002210 (Automated)	☐	☐
1.113	AZLX-23-002215 (Automated)	☐	☐
1.114	AZLX-23-002220 (Automated)	☐	☐
1.115	AZLX-23-002225 (Automated)	☐	☐
1.116	AZLX-23-002230 (Automated)	☐	☐
1.117	AZLX-23-002235 (Automated)	☐	☐
1.118	AZLX-23-002240 (Automated)	☐	☐
1.119	AZLX-23-002245 (Automated)	☐	☐
1.120	AZLX-23-002250 (Automated)	☐	☐
1.121	AZLX-23-002255 (Automated)	☐	☐
1.122	AZLX-23-002260 (Automated)	☐	☐
1.123	AZLX-23-002265 (Automated)	☐	☐
1.124	AZLX-23-002270 (Automated)	☐	☐
1.125	AZLX-23-002275 (Automated)	☐	☐
1.126	AZLX-23-002280 (Automated)	☐	☐
1.127	AZLX-23-002285 (Automated)	☐	☐
1.128	AZLX-23-002290 (Automated)	☐	☐
1.129	AZLX-23-002295 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	AZLX-23-002300 (Automated)	☐	☐
1.131	AZLX-23-002305 (Automated)	☐	☐
1.132	AZLX-23-002315 (Automated)	☐	☐
1.133	AZLX-23-002320 (Automated)	☐	☐
1.134	AZLX-23-002325 (Automated)	☐	☐
1.135	AZLX-23-002330 (Automated)	☐	☐
1.136	AZLX-23-002335 (Automated)	☐	☐
1.137	AZLX-23-002340 (Automated)	☐	☐
1.138	AZLX-23-002345 (Automated)	☐	☐
1.139	AZLX-23-002350 (Automated)	☐	☐
1.140	AZLX-23-002355 (Automated)	☐	☐
1.141	AZLX-23-002360 (Automated)	☐	☐
1.142	AZLX-23-002365 (Automated)	☐	☐
1.143	AZLX-23-002370 (Automated)	☐	☐
1.144	AZLX-23-002375 (Automated)	☐	☐
1.145	AZLX-23-002380 (Automated)	☐	☐
1.146	AZLX-23-002385 (Automated)	☐	☐
1.147	AZLX-23-002390 (Automated)	☐	☐
1.148	AZLX-23-002395 (Automated)	☐	☐
1.149	AZLX-23-002396 (Automated)	☐	☐
1.150	AZLX-23-002400 (Automated)	☐	☐
1.151	AZLX-23-002405 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	AZLX-23-002410 (Automated)	☐	☐
1.153	AZLX-23-002415 (Manual)	☐	☐
1.154	AZLX-23-002420 (Automated)	☐	☐
1.155	AZLX-23-002425 (Automated)	☐	☐
1.156	AZLX-23-002430 (Automated)	☐	☐
1.157	AZLX-23-002435 (Manual)	☐	☐
1.158	AZLX-23-002440 (Automated)	☐	☐
1.159	AZLX-23-002445 (Automated)	☐	☐
1.160	AZLX-23-002450 (Automated)	☐	☐
1.161	AZLX-23-002455 (Automated)	☐	☐
1.162	AZLX-23-002460 (Automated)	☐	☐
1.163	AZLX-23-002465 (Automated)	☐	☐
1.164	AZLX-23-002470 (Automated)	☐	☐
1.165	AZLX-23-002475 (Manual)	☐	☐
1.166	AZLX-23-002480 (Automated)	☐	☐
1.167	AZLX-23-002485 (Automated)	☐	☐
1.168	AZLX-23-002489 (Automated)	☐	☐
1.169	AZLX-23-002490 (Automated)	☐	☐
1.170	AZLX-23-002495 (Automated)	☐	☐
1.171	AZLX-23-002500 (Automated)	☐	☐
1.172	AZLX-23-002505 (Automated)	☐	☐
1.173	AZLX-23-002510 (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	AZLX-23-002515 (Automated)	☐	☐
1.175	AZLX-23-002520 (Automated)	☐	☐
1.176	AZLX-23-002535 (Automated)	☐	☐
1.177	AZLX-23-002540 (Automated)	☐	☐
1.178	AZLX-23-002555 (Automated)	☐	☐
1.179	AZLX-23-002560 (Manual)	☐	☐
1.180	AZLX-23-002565 (Manual)	☐	☐
1.181	AZLX-23-002570 (Automated)	☐	☐
1.182	AZLX-23-002575 (Automated)	☐	☐
1.183	AZLX-23-002580 (Automated)	☐	☐
1.184	AZLX-23-002590 (Automated)	☐	☐
1.185	AZLX-23-002585 (Automated)	☐	☐
1.186	AZLX-23-002595 (Automated)	☐	☐
1.187	AZLX-23-002600 (Automated)	☐	☐
1.188	AZLX-23-002605 (Manual)	☐	☐
1.189	AZLX-23-002610 (Automated)	☐	☐
1.190	AZLX-23-002615 (Automated)	☐	☐
1.191	AZLX-23-002620 (Automated)	☐	☐
1.192	AZLX-23-005000 (Automated)	☐	☐

Internal Only - General

Appendix: Change History

Date	Version	Changes for this version
3/31/2026	1.0.0	Published

Internal Only - General