CIS IBM zSecure Suite STIG Benchmark

V1.0.0 - 08-07-2025

Terms of Use

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

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

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

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

Table of Contents

Overview

Target Technology Details

IBM zSecure Suite Secure Technical Implementation Guide (STIG)

Version: 1 Release: 3 Benchmark

Date: 02 Apr 2025

Intended Audience

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

The Rule Title from the STIG.

Rationale Statement

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

Audit Procedure

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

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.

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.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for IBM zSecure Suite

Recommendations

1 STIG RULES

IBM zSecure Suite

IBM zSecure Suite Secure Technical Implementation Guide (STIG)

Version: 1 Release: 3 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 ZSEC-00-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to IBM Security zSecure installation data sets must be properly restricted and logged.

```
GROUP ID: V-259728
RULE ID: SV-259728r1050748
```

Rationale:

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

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

Audit:

Verify the accesses to zSecure installation data sets are properly restricted.

- The RACF profile(s) protecting zSecure installation data sets must not allow general access by means of UACC, ID(*), WARNING, or global access.
- The RACF profile(s) protecting zSecure installation data sets must restrict READ access to auditors, security administrators , decentralized security administrators, batch jobs that perform External Security Manager (ESM) maintenance, and trusted STC users.
- The RACF profile(s) protecting zSecure installation data sets must restrict UPDATE and higher access to systems programmers.
- All failures and successful UPDATE and higher access must be logged.

If all of the above restrictions are true, this is not a finding.

Remediation:

Ensure ALTER access to zSecure installation data sets is restricted to systems programmers, and all failures and successful UPDATE and higher access is logged.

READ access can be permitted to auditors, security administrators (domain level and decentralized), batch jobs that perform ESM maintenance, and trusted STC users.

The installing systems programmer will identify and document the product data sets and categorize them according to who will require UPDATE and higher access and if required that all successful UPDATE and higher access is logged. The installing systems programmer will identify if any additional groups need READ access for specific zSecure installation data sets, and once documented will work with the information system security officer (ISSO) to ensure they are properly restricted to the ESM active on the system.

The following commands are provided as a RACF sample for implementing zSecure installation data set controls. Please convert these commands for any other ESM:

ad 'hlq.zsec.inst.dsn' uacc(none) owner(zSecure owner) -

audit(success(update) failures(read))

pe 'hlq.zsec.inst.dsn' id(AUDTAUDT, SECAAUDT, SECBAUDT, SECDAUDT, TSTCAUDT) access(READ)

pe 'hlq.zsec.inst.dsn' id(SYSPAUDT) access(ALTER)

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)

1.2 ZSEC-00-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to IBM Security zSecure STC data sets must be properly restricted and logged.

```
GROUP ID: V-259729
RULE ID: SV-259729r960960
```

Rationale:

IBM Security zSecure STC have the ability to use privileged functions and/or have access to sensitive data. Failure to properly restrict access to these zSecure STC data sets could result in violating the integrity of the base product, which could compromise the operating system or sensitive data.

Audit:

Verify that access to the zSecure STC data sets is properly restricted.

If the following guidance is true, this is not a finding.

- The RACF profiles protecting zSecure STC data sets do not allow general access by means of UACC, ID(*), WARNING, or global access.
- READ and higher access to zAlert CKFREEZE data sets is restricted to trusted STC users and systems programmers.
- READ access to Access Monitor output data sets is restricted to auditors, decentralized security administrators, security administrators, automated operation STCs/batch jobs, batch jobs performing ESM maintenance, trusted STC users, and systems programmers.
- UPDATE access to Access Monitor output data sets is restricted to automated operation STCs/batch jobs, batch jobs performing ESM maintenance, trusted STC users, and systems programmers.
- CONTROL and higher access to Access Monitor output data sets is restricted to trusted STC users and systems programmers.
- All failures and successful UPDATE and higher access to zSecure STC data sets is logged.

DASD-only CKXLOG log stream resources in the LOGSTRM class:

- READ is restricted to security administrators, auditors, batch jobs performing ESM maintenance
- ALTER restricted to CKXLOG task, system programmers, and batch jobs performing ESM maintenance

- For Coupling-Facility CKXLOG log streams, the above applies in addition to checking the IXLSTR.model_structure_name profiles in the FACILITY class:

- UPDATE and higher trusted STC users, and systems programmers.

Remediation:

Ensure that READ and higher access to zSecure STC data sets is restricted to authorized users, and all failures and successful UPDATE and higher access is logged.

Appropriate access can be permitted to auditors, decentralized security administrators, security administrators, automated operation STCs/batch jobs, batch jobs performing ESM maintenance, trusted STC users and systems programmers.

The following commands are provided as a sample for implementing zSecure STC data set controls:

```
ad 'hlq.zsec.alert.ckfreeze' uacc(none) owner(zSecure owner) -
audit(success(update) failures(read))
pe 'hlq.zsec.alert.ckfreeze' id(SYSPAUDT, TSTCAUDT) access(READ)
ad 'hlq.zsec.access.monitor.dsn' uacc(none) owner(zSecure owner) -
audit(success(UPDATE) failures(READ))
pe 'hlq.zsec.access.monitor.dsn' id(AUDTAUDT, SECAAUDT, SECDAUDT, SECBAUDT)
access(READ)
pe 'hlq.zsec.access.monitor.dsn' id(SECBAUDT,
access(UPDATE)
pe 'hlq.zsec.access.monitor.dsn' id(SYSPAUDT, TSTCAUDT) access(ALTER)
rdef logstrm LSName uacc(none) owner(zSecure owner) - audit(success(UPDATE)
failures(read))
pe LSName class(logstrm) id(AUDTAUDT, SECAAUDT, SECDAUDT) access(READ)
pe LSName class(logstrm) id(CKXLOG, SECBAUDT, AUTOAUDT, SYSPAUDT)
access(ALTER)
rdef facility IXLSTR. <modelstrname> uacc(none) owner(zSecure owner) -
audit(success(UPDATE) failures(READ))
pe IXLSTR.<modelstrname> class(facility) id(SYSPAUDT, TSTCAUDT) access(ALTER)
```

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)

1.3 ZSEC-00-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to IBM Security zSecure user data sets must be properly restricted and logged.

```
GROUP ID: V-259730
RULE ID: SV-259730r1050750
```

Rationale:

If zSecure were to allow inappropriate reading or updating of user data sets, sensitive information could be disclosed, or changes might result in incorrect results reported by the product. Only qualified and authorized individuals must be allowed to create, read, update, and delete zSecure user data sets.

Audit:

Verify the accesses to the zSecure user data sets are properly restricted. If the following guidance is true, this is not a finding.

- The RACF profiles protecting zSecure user data sets do not allow general access by means of UACC, ID(*), WARNING, or global access.
- READ access to ASSERTION, CKFREEZE, and UNLOAD data sets is restricted to auditors, automated operation STCs/batch jobs, decentralized security administrators, security administrators, batch jobs performing ESM maintenance, system programmers and trusted STC users.
- UPDATE and higher access to ASSERTION, CKFREEZE, and UNLOAD data sets is restricted to decentralized security administrators, security administrators, batch jobs performing ESM maintenance, and system programmers.
- All failures and successful UPDATE and higher access to ASSERTION, CKFREEZE, and UNLOAD data sets is logged.
- READ access to Access Monitor output data sets is restricted to auditors, decentralized security administrators, security administrators, batch jobs performing ESM maintenance, automated operation STCs/batch jobs, and trusted STC users, and system programmers.
- UPDATE and higher access to the Access Monitor output data sets is restricted to automated operation STCs/batch jobs, batch jobs performing ESM maintenance, trusted STC users, and system programmers.
- All failed and all successful UPDATE and higher access to Access Monitor output data sets is logged.
- READ access to CKACUST and CKACUSV data sets is restricted to auditors, batch jobs that perform ESM maintenance, decentralized security administrators, security administrators, automated operation STCs/batch jobs, trusted STC users, and systems programmers.
- UPDATE access to CKACUST and CKACUSV data sets is restricted to decentralized security administrators, security administrators, automated operation STCs/batch jobs, batch jobs performing ESM maintenance, trusted STC users, and systems programmers.
- CONTROL and higher access to CKACUST and CKACUSV data sets is restricted to systems programmers.
- All failed and all successful UPDATE and higher access to CKACUST and CKACUSV data sets is logged.
- READ access to CKXLOG log stream is restricted to auditors, decentralized security administrators, security administrators, automated operation STCs/batch jobs, trusted STC users, and system programmers.
- UPDATE and higher access to CKXLOG log stream is restricted to automated operation STCs/batch jobs, trusted STC users, and system programmers.
- All failed access to CKXLOG log stream is logged.

Remediation:

The following commands are provided as a RACF sample for implementing zSecure user data set controls. Convert these commands for any other ESM:

```
ad 'hlq.zsec.user.assert/ckfreeze/unload.dsn' uacc(none) owner(zSecure owner)
-
audit(success(update) failures(read))

pe 'hlq.zsec.user.assert/ckfreeze/unload.dsn' id(AUDTAUDT, AUTOAUDT,
SECAAUDT, SECDAUDT, SECBAUDT, TSTCAUDT) access(READ)

pe 'hlq.zsec.user.assert/ckfreeze/unload.dsn' id(SECAAUDT, SECDAUDT,
SECBAUDT, SYSPAUDT) access(ALTER)

ad 'hlq.zsec.accmon.user.dsn' uacc(none) owner(zSecure owner) -
audit(success(update) failures(read))

pe 'hlq.zsec.accmon.user.dsn' id(AUDTAUDT, AUTOAUDT, SECAAUDT, SECDAUDT,
SECBAUDT, TSTCAUDT) access(READ)

pe 'hlq.zsec.accmon.user.dsn' id(AUTOAUDT, SECBAUDT, TSTCAUDT, SYSPAUDT)
access(ALTER)
ad ' hlq.zsec.user.ckcus*
audit(success(UPDATE) failures(READ))

pe 'hlq.zsec.user.ckcus*' id(AUDTAUDT, AUTOAUDT, SECAAUDT, SECDAUDT,
SECBAUDT, TSTCAUDT) access(UPDATE)

pe 'hlq.zsec.user.ckcus*' id(SYSPAUDT) access(ALTER)
rdef logstrm LSName uacc(none) owner(zSecure owner) -
audit(success(UPDATE) failures(read))

pe LSName class(logstrm) id(AUDTAUDT, AUTOAUDT, SECAAUDT, SECDAUDT, TSTCAUDT,
SYSPAUDT) access(READ)
pe LSName class(logstrm) id(AUTOAUDT, TSTCAUDT, SYSPAUDT) access(ALTER)
```

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)

1.4 ZSEC-00-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Started tasks for IBM Security zSecure products must be properly defined.

```
GROUP ID: V-259731
RULE ID: SV-259731r1051324
```

Rationale:

Started tasks and batch job IDs can be automatically revoked accidentally if not properly protected. When properly protected STCs prevent any attempts to log on with a password, it eliminates the possibility of revocation due to excessive invalid password attempts (denial of service).

Audit:

If user IDs assigned to zSecure started tasks and scheduled batch jobs are not assigned the PROTECTED attribute and/or defined as an STC, this is a finding.

The default zSecure STC names (that may be changed by installation) are as follows:

- STC C2PACMON runs program C2PACMON.
- STC C2POLICE runs program C2POLICE.
- STC C2PCOLL runs program CKFCOLL. (CKFCOLL is also run as a step in batch jobs.)
- STC C2RSERVE runs program BPXBATCH.
- STC CKCS1154 runs program CKCS1154.
- STC CKNSERVE runs program CKNSERVE.
- STC CKCCEF runs program CKRCARLX.
- STC CKQCLEEF runs program CKRCARLX.
- STC CKQEXSMF runs program CKQEXSMF.
- STC CKQRADAR runs program CKRCARLA.
- STC CKXLOG runs program CKXLOG.

Verify the naming conventions for the zSecure STCs and batch jobs with the responsible systems programmers.
Check which user IDs are assigned in the STDATA segment of the zSecure STCs. For these user IDs, verify they are assigned the PROTECTED attribute.

Remediation:

Ensure user IDs assigned to zSecure started tasks and scheduled batch jobs are assigned the PROTECTED attribute and/or defined as an STC.

The following command is provided as a sample for adding the PROTECTED attribute. Convert this command for any other ESM:

- ALTUSER NOPASSWORD NOPHRASE
- ALTUSER <batch user ID> NOPASSWORD NOPHRASE

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

1.5 ZSEC-00-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to IBM Security zSecure program resources must be limited to authorized users.

```
GROUP ID: V-259732
RULE ID: SV-259732r961095
```

Rationale:

Functional access (which is controlled with access to XFACILIT profiles) must not commingle multiple functions under a single resource profile.

Audit:

If the profiles protecting zSecure program resources do not allow general access by means of UACC, ID(*),WARNING, or global access, this is not a finding.

Review profile(s) protecting CKF.** resources in XFACILIT class.

If READ and higher access to any other CKF. profiles is not restricted to security administrators, decentralized security administrators, security batch jobs performing External Security Manager (ESM) maintenance, and trusted STC users, this is a finding.

Review profile(s) protecting CKN*.** resources in XFACILIT class.

If READ and higher access to any other CKNADMIN.**, and CKNDSN.**, profiles is not restricted to security administrators, decentralized security administrators, security batch jobs performing ESM maintenance, and trusted STC users, this is a finding.

Review profile(s) protecting CKG.** resources in XFACILIT class.

If READ and higher access to any other CKG.CMD.**, CKG.RAC.**, CKG.SCHEDULE.**, CKG.SCP.**, CKG.SCPASK.**,CKG.UCAT.**, or CKG.USRDATA.** profiles is not restricted to security administrators, decentralized security administrators, security batch jobs performing ESM maintenance, and trusted STC users, this is a finding.

Review profile(s) protecting CKR.** resources in XFACILIT class.

If READ and higher access to any other CKR.ACTION.**, CKR.CKRCARLA.APF, CKR.CKXLOG.**, CKR.OPTION.**, or CKR.READALL profiles is not restricted to security administrators, decentralized security administrators, security batch jobs performing ESM maintenance, and trusted STC users, this is a finding.

If zSecure is used, review profile(s) protecting C2R.** resources in XFACILIT class.

If READ and higher access to any other C2R.CLIENT.** or C2R.SERVER.ADMIN profiles is not restricted to security administrators, decentralized security administrators, security batch jobs performing ESM maintenance, and trusted STC users, this is a finding.

Review profile(s) protecting C2X.** resources in XFACILIT class.

If UPDATE access to any other C2X.ICH* profile is not restricted to automated operation STCs/batch jobs or trusted STC users, this is a finding.

If all failures and successful UPDATE and higher access attempts are logged, this is not a finding.

Remediation:

Ensure READ and higher access to zSecure program resources is restricted to the appropriate staff members.

READ and higher access can be given to security administrators, decentralized security administrators, security batch jobs that perform ESM maintenance, and trusted STC users.

The following commands are provided as a sample for implementing zSecure functional resource controls:

```
rdef CKF.<focus> uacc(none) owner(zSecure owner)
pe CKF.<focus> class(XFACILIT) id(SECAAUDT, SECBAUDT, SECDAUDT, TSTCAUDT)
access(READ)
rdef xfacilit CKNADMIN.<type>.<node-name> uacc(none) owner(zSecure owner)
pe CKNADMIN.<type>.<node-name> class(xfacilit) id(SECAAUDT, SECBAUDT,
SECDAUDT, TSTCAUDT) access(READ)
rdef xfacilit CKNDSN.<dstype>.<node-name>.<systemname>.<type> uacc(none)
owner(zSecure owner)
pe CKNDSN.<dstype>.<node-name>.<systemname>.<type> class(xfacilit)
id(SECAAUDT, SECBAUDT, SECDAUDT, TSTCAUDT) access(READ)
rdef xfacilit CKG.<type>.** uacc(none) owner(zSecure owner)
pe CKG.<type>.** class(xfacilit) id(SECAAUDT, SECBAUDT, SECDAUDT, TSTCAUD)
access(READ)
rdef xfacilit CKR.<type> uacc(none) owner(zSecure owner)
pe CKR.<type>.** class(xfacilit) id(SECAAUDT, SECBAUDT, SECDAUDT, TSTCAUD)
access(READ)
rdef xfacilit C2R.SERVER.ADMIN uacc(none) owner(zSecure owner)

pe C2R.SERVER.ADMIN class(xfacilit) id(SECAAUDT, SECBAUDT, TSTCAUD)
access(READ)
rdef xfacilit C2R.CLIENT.** uacc(none) owner(zSecure owner)
pe C2R.CLIENT.** class(xfacilit) id(SECAAUDT, SECBAUDT, TSTCAUD) access(READ)
rdef xfacilit C2X.ICH* uacc(none) owner(zSecure owner)
pe C2X.ICH* class(xfacilit) id(AUTOAUDT, TSTCAUDT) access(UPDATE)
```

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

1.6 ZSEC-00-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

IBM Security zSecure must prevent nonprivileged users from executing privileged zSecure functions.

```
GROUP ID: V-259733
RULE ID: SV-259733r1050755
```

Rationale:

Preventing nonprivileged users from executing privileged zSecure functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, running COLLECT jobs, generating audit reports, and adjusting RACF security settings. Nonprivileged users are individuals who do not possess appropriate authorizations.

Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from nonprivileged users.

Audit:

If READ access to zSecure functional resources is not restricted to privileged users, this is a finding.

If the following high-level qualifier profiles are defined in the configured zSecure class, by default XFACILIT, with UACC (NONE) and not in WARNING mode, this is not a finding.

CKF.**

CKN*.**

CKG.**

CKR.**

C2R.** (if you use zSecure Visual)

C2X.**

If a minimum of all failed access is logged, this is not a finding.

Remediation:

Ensure that the following high-level qualifier profiles are defined in the configured zSecure class, by default XFACILIT, with UACC (NONE) and not in WARNING mode:

CKF.**

CKN*.**

CKG.**

CKR.**

C2R.** (if you use zSecure Visual)

C2X.**

A minimum of all failed access must be logged.

The following is an example of RACF commands. Convert these commands for any other ESM:

```
rdef xfacilit CKF.** uacc(none) owner(zSecure owner)
rdef xfacilit CKN*.** uacc(none) owner(zSecure owner)
rdef xfacilit CKG.** uacc(none) owner(zSecure owner)
rdef xfacilit CKR.** uacc(none) owner(zSecure owner)
rdef xfacilit C2R.** uacc(none) owner(zSecure owner)
rdef xfacilit C2X.** uacc(none) owner(zSecure owner)
```

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)

1.7 ZSEC-00-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The IBM Security zSecure programs CKFCOLL and CKGRACF, and the APF-authorized version of program CKRCARLA, must be restricted to security administrators, security batch jobs performing External Security Manager (ESM) maintenance, auditors, and systems programmers, and must be audited.

```
GROUP ID: V-259734
RULE ID: SV-259734r1050758
```

Rationale:

Users authorized to use the zSecure program CKFCOLL can collect z/OS system information that is not accessible to regular users.

Users authorized to use the zSecure program CKGRACF can change certain permitted RACF profile definitions that otherwise would not be allowed.

Users authorized to use the zSecure program CKRCARLX can fake SMF records.

Allowing inappropriate users to use the CKFCOLL, CKGRACF, and CKRCARLX programs could result in disclosure of z/OS installation and configuration information or inappropriate RACF profile or SMF record changes.

Satisfies: SRG-APP-000342-MFP-000090,SRG-APP-000343-MFP-000091

Audit:

If this is not a RACF system, the presence of CKGRACF is not applicable.

Verify the access and log settings of the profiles that protect the use of the CKFCOLL and CKGRACF programs and the APF-authorized version of the CKRCARLA program.

If the CKF.** and CKG.** profiles that protect the use of the CKFCOLL, CKGRACF, and CKRCARLA programs allow general access (UACC, ID(*), WARNING, or global access) or do not log successful READ access, this is a finding.

If READ or higher access to profile(s) protecting CKF.** resources in XFACILIT class is not restricted to security administrators (domain or decentralized), batch jobs performing ESM maintenance, auditors, or systems programmers, this is a finding.

If READ or higher access to profile(s) protecting CKG.** resources in XFACILIT class is not restricted to security administrators (domain or decentralized) or batch jobs performing ESM maintenance, this is a finding.

Review auditing of the profile protecting the CKR.CKRCARLA.APF resource in XFACILIT class.

If successful READs are not audited, this is a finding.

Remediation:

The following commands are provided as a sample for implementing RACF zSecure user data set controls. Convert these commands for any other ESM:

```
rdef program CKFCOLL uacc(none) owner(zSecure owner) audit(all(read))
pe CKFCOLL class(program) id(AUDTAUDT, SECAAUDT, SECBAUDT,
SECDAUDT, SYSPAUDT) access(READ)
rdef program CKGRACF uacc(none) owner(zSecure owner) audit(all(read))
pe CKGRACF class(program) id(AUDTAUDT, SECAAUDT, SECBAUDT,
SECDAUDT, SYSPAUDT) access(READ)
rdef program CKRCARLX uacc(none) owner(zSecure owner) audit(all(read))
pe CKRCARLX class(program) id(AUDTAUDT, SECAAUDT, SECBAUDT,
SECDAUDT, SYSPAUDT) access(READ)
```

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)

1.8 ZSEC-00-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

IBM Security zSecure must implement organization-defined automated security responses if baseline zSecure configurations are changed in an unauthorized manner.

```
GROUP ID: V-259735
RULE ID: SV-259735r961458
```

Rationale:

Unauthorized changes to the zSecure baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the system. Changes to information system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the application. Examples of security responses include but are not limited to the following: halting application processing, halting selected application functions, or issuing alerts/notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Audit:

Verify that a (daily) scheduled batch job is defined and used or a custom alert is configured and activated to inform appropriate personnel, such as auditors and compliance officers, about successful changes to the zSecure configuration data sets on their z/OS systems.

If SMF records regarding successful UPDATE(s) to zSecure configuration data sets are not reported to the information system security manager (ISSM), this is a finding.

Remediation:

The recipients of the SMF reports or alert messages must investigate whether the UPDATE is legitimate (e.g., is documented and approved in a change management request). If it is not, they must restore the original configuration setting.

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)

1.9 ZSEC-00-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

IBM Security zSecure must remove all upgraded/replaced zSecure software components that are no longer required for operation after updated versions have been installed.

```
GROUP ID: V-259736
RULE ID: SV-259736r961677
```

Rationale:

Previous versions of zSecure products and components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

Examine the inventory of installed software components for zSecure.

If software components that are no longer required for operation exist, this is a finding.

Remediation:

Remove all upgraded/replaced software components that are no longer required for operation.

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)

1.10 ZSEC-00-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

IBM Security zSecure system administrators must install security-relevant zSecure software updates within the time period directed by an authoritative source (e.g., IAVMs, CTOs, DTMs, and STIGs).

```
GROUP ID: V-259737
RULE ID: SV-259737r961683
```

Rationale:

Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

Audit:

Ask the system administrator for the procedure to install security-relevant software updates within the time period directed by an authoritative source (e.g., IAVMs, CTOs, DTMs, and STIGs.

If there is no procedure, this a finding.

Remediation:

Develop a procedure to install security-relevant software updates within the time period directed by an authoritative source (e.g., IAVMs, CTOs, DTMs, and STIGs).

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

1.11 ZSEC-00-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

XFACILIT class, or alternate class if specified in module CKRSITE, must be active.

```
GROUP ID: V-259738
RULE ID: SV-259738r961863
```

Rationale:

The zSecure resource class that is configured for the zSecure access checks must be active to receive valid Allow/Deny responses from external security manager (ESM) resource checks. Activation is outside of zSecure, in the ESM.

Audit:

Run the CARLa command SHOW CKRSITE. The output of this command reveals which resource class is configured for handling the zSecure security checks. The default resource class is XFACILIT.

Verify in the class descriptor table that the configured zSecure resource class is active.

If the configured zSecure resource class is not active, this is a finding.

Remediation:

Ensure the resource class that is configured in CKRSITE for zSecure security checks is active in the RACF class descriptor table. The default class is XFACILIT. IBM Security zSecure recommends the generic be activated.

Following is a sample command:

SETROPTS CLASSACT(XFACILIT) or SETROPTS CLASSACT()

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	ZSEC-00-000040 (Manual)	☐	☐
1.2	ZSEC-00-000060 (Manual)	☐	☐
1.3	ZSEC-00-000080 (Manual)	☐	☐
1.4	ZSEC-00-000100 (Manual)	☐	☐
1.5	ZSEC-00-000120 (Manual)	☐	☐
1.6	ZSEC-00-000140 (Manual)	☐	☐
1.7	ZSEC-00-000160 (Manual)	☐	☐
1.8	ZSEC-00-000200 (Manual)	☐	☐
1.9	ZSEC-00-000220 (Manual)	☐	☐
1.10	ZSEC-00-000240 (Manual)	☐	☐
1.11	ZSEC-00-000260 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08/07/2025	1.0.0	Initial CIS Release