

CIS IBM z/OS V2R5 with RACF Benchmark

v1.0.0 - 05-20-2022

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/>

Table of Contents

| | |
|---|-----------|
| Terms of Use | 1 |
| Table of Contents | 2 |
| Overview | 9 |
| Intended Audience..... | 9 |
| Consensus Guidance | 10 |
| Typographical Conventions..... | 11 |
| Recommendation Definitions..... | 12 |
| Title | 12 |
| Assessment Status..... | 12 |
| Automated | 12 |
| Manual..... | 12 |
| Profile | 12 |
| Description..... | 12 |
| Rationale Statement | 12 |
| Impact Statement..... | 13 |
| Audit Procedure..... | 13 |
| Remediation Procedure..... | 13 |
| Default Value..... | 13 |
| References | 13 |
| CIS Critical Security Controls® (CIS Controls®)..... | 13 |
| Additional Information..... | 13 |
| Profile Definitions | 14 |
| Acknowledgements | 15 |
| Recommendations | 16 |
| 1 Identification and Authentication | 16 |
| 1.1 Password Control | 17 |
| 1.1.1 Ensure that the PASSWORD(INTERVAL) SETROPTS value is set to no longer than 90 days (Automated) | 18 |
| 1.1.2 Ensure that the PASSWORD(HISTORY) SETROPTS value is set to at least 4 (Automated) | 20 |
| 1.1.3 Ensure that the PASSWORD(RULEn) SETROPTS value(s) is set (Automated) | 22 |
| 1.1.4 Ensure that the SETROPTS PASSWORD(MINCHANGE(n)) value will specified a value greater the zero (0) (Automated) | 24 |
| 1.1.5 Ensure that the PASSWORD(REVOKE) SETROPTS value is specified (Automated) | 26 |
| 1.1.6 Ensure that the KDFAES algorithm is used to protect passwords in the security database (Automated) | 28 |
| 1.1.7 Ensure that the PASSWORD(WARNING) SETROPTS value is set (Automated) | 30 |
| 1.2 System Settings | 31 |

| | |
|--|------------|
| 1.2.1 Ensure that Inactive users are revoked (Automated) | 32 |
| 1.2.2 Ensure that STARTED class is used to assign users to Started Tasks (Automated) | 34 |
| 1.2.3 Ensure user propagation is protected with the PROPCNTL class (Automated) | 36 |
| 1.2.4 Ensure that Job wait time option is set (Automated) | 38 |
| 1.2.5 Ensure that started tasks defined with the trusted attribute are justified (Manual) | 39 |
| 1.2.6 Ensure that the OPERCMDS resource class is ACTIVE and RACLISTed (Automated) | 41 |
| 1.2.7 Ensure that CONSOLE resource class is ACTIVE (Manual) | 43 |
| 1.2.8 Ensure that FACILITY resource class is ACTIVE and RACLISTED (Automated) | 45 |
| 1.2.9 Ensure that inapplicable PPT entries have been invalidated (Manual) | 47 |
| 1.2.10 Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) currently active parmlib data set(s) (Automated) | 49 |
| 1.2.11 Ensure that the CONSOLxx members are configured (Manual) | 51 |
| 1.2.12 Ensure that no expired digital certificates are used (Automated) | 53 |
| 1.2.13 Ensure that RACF RVARYPW are set to non-default values (Automated) | 54 |
| 1.3 User Attributes | 56 |
| 1.3.1 Ensure that the use of RACF SPECIAL Attribute is justified (Manual) | 57 |
| 1.3.2 Ensure that SYS1.UADS contains only emergency use user IDs (Manual) | 59 |
| 1.3.3 Ensure that MCS console user ID(s) is protected (Manual) | 61 |
| 1.3.4 Ensure that all STARTED class profiles specify PROTECTED user IDs (Automated) | 63 |
| 2 Authorization and Access Control Management | 65 |
| 2.1 Data Protection | 66 |
| 2.1.1 Ensure that Maintenance user IDs are protected (Manual) | 67 |
| 2.1.2 Ensure that access to active SMF collection files is controlled (Automated) | 69 |
| 2.1.3 Ensure that the WHEN(PROGRAM) SETROPTS value is active (Automated) | 70 |
| 2.1.4 Ensure that the ICHDSM00 program is protected (Automated) | 72 |
| 2.1.5 Ensure that the IRRDPI00 program is protected (Automated) | 74 |
| 2.1.6 Ensure that the SETROPTS ERASE value is set to ERASE(ALL) on all systems (Automated) | 76 |
| 2.1.7 Ensure that the TEMPDSN class is active (Automated) | 78 |
| 2.1.8 Ensure the RACF security data sets and all copies are protected (Automated) | 80 |
| 2.1.9 Ensure the RACF remote sharing facility files are protected (Automated) | 82 |
| 2.1.10 Ensure the RACF parameter library file is protected (Automated) | 85 |
| 2.1.11 Ensure that RACF remote sharing connections use the TCP/IP protocol (Automated) | 87 |
| 2.1.12 Ensure that memory and privileged program dumps are protected (Automated) | 89 |
| 2.1.13 Ensure that access to system trace datasets is controlled (Automated) | 91 |
| 2.1.14 Ensure that access to system backup datasets is controlled (Automated) | 93 |
| 2.1.15 Ensure that access to SYSTEM DUMP data sets is controlled (Automated) | 95 |
| 2.1.16 Ensure that access to SMF collection offload datasets is controlled (Automated) | 97 |
| 2.1.17 ENSURE that Temporary Data Sets are protected (Automated) | 99 |
| 2.2 Resource Protection | 101 |
| 2.2.1 Ensure that the ability to update system dynamic lists are protected (Automated) | 102 |
| 2.2.2 Ensure that the GENERIC SETROPTS value is enabled for ACTIVE classes (Automated) | 104 |
| 2.2.3 Ensure that IEASYMUP resource is protected (Manual) | 106 |
| 2.2.4 Ensure that PASSWORD protection for data sets is not used (Manual) | 108 |
| 2.2.5 Ensure that access to datasets in the PARMLIB concatenation is controlled (Automated) | 109 |
| 2.2.6 Ensure that access to all LPA libraries is controlled (Manual) | 111 |
| 2.2.7 Ensure that access to the System Master Catalog is controlled (Manual) | 112 |
| 2.2.8 Ensure that access to all APF-authorized objects is controlled (Manual) | 114 |
| 2.2.9 Ensure that access to SYS1.SVCLIB is controlled (Automated) | 116 |
| 2.2.10 Ensure that access to SYS1.IMAGELIB is controlled (Manual) | 118 |
| 2.2.11 Ensure that access to libraries that contain PPT modules is controlled (Automated) | 120 |
| 2.2.12 Ensure that access to SYS1.NUCLEUS is controlled (Manual) | 122 |
| 2.2.13 Ensure that access to all system PROCLIB data sets is controlled (Automated) | 124 |

| | |
|---|------------|
| 2.2.14 Ensure that System REXX data set is protected (Automated) | 126 |
| 2.2.15 Ensure that Access to SYS1.LINKLIB is protected (Automated)..... | 128 |
| 2.2.16 Ensure that access to all system-level product installation libraries is controlled (Automated) | 130 |
| 2.3 System Settings | 131 |
| 2.3.1 Ensure that the TERMINAL SETROPTS value is set to NONE (Automated)..... | 132 |
| 2.3.2 Ensure that the GENCMD SETROPTS value is enabled for ACTIVE classes (Automated) | 134 |
| 2.3.3 Ensure that the PROTECTALL SETROPTS value is set to FAIL (Automated) | 136 |
| 2.4 User Privilege | 138 |
| 2.4.1 Ensure that the assignment of the RACF OPERATIONS attribute is tightly controlled (Automated)..... | 139 |
| 2.4.2 Ensure that TSOAUTH resources are restricted to authorized users (Automated) | 141 |
| 2.4.3 Ensure that access for Surrogate users is controlled (Automated) | 143 |
| 2.4.4 Ensure that UID 0 is only assigned to PROTECTED STC IDs (Automated) | 145 |
| 2.4.5 Ensure that started tasks requiring exceptional access rights use the TRUSTED attribute and (Automated) | 147 |
| 2.4.6 Ensure that access to Libraries containing EXIT modules is controlled (Automated) | 149 |
| 2.4.7 Ensure that access to LINKLIST libraries is controlled (Automated) | 151 |
| 2.4.8 Ensure that access to SYS1.UADS is maintained (Automated) | 153 |
| 2.4.9 Ensure that Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) is controlled (Automated) | 155 |
| 2.4.10 Ensure that MCS consoles access is protected through CONSOLE CLASS profile (Manual) | 156 |
| 2.4.11 Ensure that access to CONSOLE resources for users in TSOAUTH resource class is restricted (Automated) | 158 |
| 2.4.12 Ensure that access to system user catalogs is controlled (Automated) | 160 |
| 3 Logging and Auditing | 161 |
| 3.1 Ensure that the command violations are being logged (Automated) | 162 |
| 3.2 Ensure that activity of SPECIAL users are being logged (Automated)..... | 164 |
| 3.3 Ensure that the AUDIT SETROPTS value is set for all classes (Automated)..... | 166 |
| 3.4 Ensure that activities of users with the OPERATIONS attribute are logged (Automated) | 168 |
| 3.5 Ensure that Logon statistics are recorded (Automated) | 170 |
| 3.6 Ensure RACF AUDITOR or ROAUDIT privilege is assigned only to users with auditing mission. (Automated) | 172 |
| 3.7 Ensure that effective SMF records collection options are set (Automated) | 173 |
| 3.8 Ensure that an automated process is in place to collect and retain SMF data (Manual) | 175 |
| 3.9 Ensure that Required SMF data record types is collected (Automated)..... | 177 |
| 3.10 Ensure that RACF audit logs is reviewed on a regular basis (Manual) | 180 |
| 3.11 Ensure regular audit of AC=1 modules in APF authorized libraries are conducted (Manual)..... | 181 |
| 3.12 Ensure that only supported (vendor) system software is installed and active on the system (Manual) | 182 |
| 3.13 Ensure all software on your system is supported (Manual)..... | 183 |
| 3.14 Implement sensitive z/OS datasets monitoring (Manual) | 184 |
| 4 System Resilience | 185 |
| 4.1 Ensure that RACF database is backed up on a scheduled basis (Manual)..... | 186 |
| 4.2 Ensure that RACF primary and backup databases are isolated (Manual) | 187 |
| 4.3 Ensure sensitive data is encrypted (Manual) | 189 |
| 5 Storage Management..... | 190 |
| 5.1 Ensure that DFSMS is configured (Manual)..... | 191 |
| 5.2 Ensure that a very limited number of users can use the Tape Bypass Label Processing (BLP) (Manual) | 192 |
| 5.3 Ensure that Automatic Data Set Protection (ADSP) SETROPTS value is set to NOADSP (Manual) .. | 194 |
| 5.4 Ensure that DFSMS control data sets are protected (Manual) | 195 |
| 6 Networking | 197 |

| | |
|---|------------|
| 6.1 CSSMTP Recommendations..... | 198 |
| 6.1.1 Ensure CSSMTP Started Task name is configured (Manual) | 199 |
| 6.1.2 Ensure CSSMTP Started task(s) is defined to the STARTED resource class. (Manual)..... | 201 |
| 6.1.3 Ensure AT-TLS protection is enabled for CSSMTP (Manual) | 203 |
| 6.1.4 Ensure CSSMTP STC data sets are protected. (Manual) | 206 |
| 6.2 FTP Recommendations | 208 |
| 6.2.1 Ensure FTP Server daemon is configured with proper security parameters (Manual) | 209 |
| 6.2.2 Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords (Manual)..... | 211 |
| 6.2.3 Ensure FTP.DATA configuration statements enforce secure configuration (Manual) | 214 |
| 6.2.4 Ensure AT-TLS protection is enabled for the FTP daemon (Manual) | 218 |
| 6.2.5 Ensure User exits for the FTP Server are not used without approval (Manual) | 221 |
| 6.2.6 Ensure warning banner for the FTP Server is specified (Manual) | 224 |
| 6.2.7 Ensure SMF recording options for the FTP Server are configured (Manual) | 225 |
| 6.2.8 Ensure permission and user audit bits for FTP Server are configured. (Manual) | 228 |
| 6.2.9 Ensure MVS data sets for the FTP Server are protected. (Manual) | 232 |
| 6.2.10 Ensure FTP Control cards are stored in a secure PDS file (Manual) | 234 |
| 6.3 OpenSSH | 236 |
| 6.3.1 Ensure SSH daemon is configured to only use the SSHv2 protocol (Manual) | 237 |
| 6.3.2 (Optional) Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider where required (Manual) | 239 |
| 6.3.3 Ensure SSH daemon is configured with the logon banner (Manual) | 242 |
| 6.3.4 Ensure SMF recording options for the SSH daemon are configured (Manual) | 243 |
| 6.3.5 Ensure SSH daemon is configured to use SAF keyrings for key storage (Manual) | 245 |
| 6.4 Syslogd Recommendations..... | 247 |
| 6.4.1 Ensure Syslog daemon is started at z/OS initialization (Manual) | 248 |
| 6.4.2 Ensure Syslog daemon is secured (Manual)..... | 250 |
| 6.4.3 Ensure permission and user audit bits for Syslog daemon component are configured. (Manual) | 252 |
| 6.4.4 Ensure syslogd archive data sets are protected (Manual) | 256 |
| 6.5 TCP/IP Recommendations | 258 |
| 6.5.1 Ensure configuration files for the TCP/IP stack are explicitly specified (Manual) | 259 |
| 6.5.2 Ensure TCP/IP stack configuration defined in TCPIP.DATA (Manual)..... | 261 |
| 6.5.3 Ensure Hosts identified by the NSINTERADDR statement are protected (Manual) | 263 |
| 6.5.4 Ensure PROFILE.TCPIP configuration statements for the TCP/IP stack are defined (Manual) | 264 |
| 6.5.5 Ensure permission and user audit bits for z/OS Unix file system objects that are part of the Base TCP/IP component are configured (Manual)..... | 269 |
| 6.5.6 Ensure access to TCP/IP SAF resources (Manual) | 273 |
| 6.5.7 Ensure RACF SERVAUTH resource class is active for TCP/IP resources (Manual) | 278 |
| 6.5.8 Ensure Started tasks for the base TCP/IP component are defined securely in RACF (Manual) | 280 |
| 6.5.9 Ensure MVS data sets for the Base TCP/IP component are protected (Manual) | 282 |
| 6.6 TN3270 Recommendations..... | 284 |
| 6.6.1 Ensure configuration statements for the TN3270E Telnet Server are configured. (Manual) | 285 |
| 6.6.2 Ensure VTAM session setup controls for the TN3270E Telnet Server are configured (Manual) | 289 |
| 6.6.3 Ensure Warning banner for the TN3270 Telnet Server is configured (Manual)..... | 293 |
| 6.6.4 Ensure AT-TLS protection is enabled for the TN3270 Telnet Server (Manual) | 294 |
| 6.6.5 Ensure SMF recording options for the TN3270 Telnet Server are configured (Manual) | 297 |
| 6.6.6 Ensure Startup user account for the z/OS UNIX Telnet Server is defined (Manual) | 299 |
| 6.7 VTAM Recommendations | 301 |
| 6.7.1 Ensure VTAM USSTAB definitions are being used for secured terminals (Manual) | 302 |
| 6.7.2 Ensure System datasets used to support the VTAM network are secured (Manual) | 304 |
| 7 Cryptography and Encryption | 306 |
| 7.1 ICSF Installation and Configuration..... | 307 |

| | |
|---|------------|
| 7.1.1 Ensure that all ICSF Installation Datasets are protected. (Manual) | 308 |
| 7.1.2 Ensure that the ICSF Started Task is protected (Manual) | 311 |
| 7.1.3 Ensure CSFINPV2 requires signature verification (Manual) | 313 |
| 7.1.4 Ensure ICSF is configured to start during IPL (Manual) | 315 |
| 7.2 ICSF Component Configuration | 317 |
| 7.2.1 Ensure Crypto Usage Statistics are enabled (Manual) | 318 |
| 7.2.2 Ensure Crypto Key Lifecycle Auditing is enabled (Manual) | 320 |
| 7.2.3 Ensure Crypto Key Usage Auditing is enabled (Manual) | 322 |
| 7.2.4 Ensure ICSF Key Data Sets have a system backup (Manual) | 324 |
| 7.2.5 Ensure ICSF Master Keys have a backup procedure (Manual) | 325 |
| 7.2.6 Ensure all ICSF Key Data Sets are in Common Record Format (Manual) | 327 |
| 7.2.7 Ensure all ICSF Key Data Sets are enabled for sysplex sharing (Manual) | 329 |
| 7.2.8 Ensure ICSF is running with FIPSMODE enabled (Manual) | 331 |
| 7.2.9 Ensure CCA Operational Keys Are Created with WRAPENH3 Key Wrapping (Manual) | 333 |
| 7.3 ICSF Security Configuration | 335 |
| 7.3.1 Ensure CSFSERV class is active (Manual) | 336 |
| 7.3.2 Ensure CSFKEYS class is active (Manual) | 338 |
| 7.3.3 Ensure CRYPTOZ class is active (Manual) | 340 |
| 7.3.4 Ensure the XCSFKEY class is active (Manual) | 342 |
| 7.3.5 Ensure ICSF Key Store Policy controls are enabled (Manual) | 343 |
| 7.3.6 Ensure ICSF Key Datasets are protected (Manual) | 345 |
| 7.3.7 Ensure ICSF administrative services are protected (Manual) | 347 |
| 7.3.8 Ensure ICSF operator commands are protected (Manual) | 349 |
| 8 Job Management JES2 | 351 |
| 8.1 JES2 Commands | 352 |
| 8.1.1 Ensure that JES2 system commands are protected (Manual) | 353 |
| 8.2 JES2 SPOOL | 355 |
| 8.2.1 Ensure that JESSPOOL CLASS is active (Manual) | 356 |
| 8.2.2 Ensure that JES2 spool resources are protected (Manual) | 357 |
| 8.2.3 Ensure that JES2 trace resources are protected (Manual) | 361 |
| 8.2.4 Ensure that JESNEWS resources are protected (Manual) | 363 |
| 8.3 Job Level Protection | 365 |
| 8.3.1 Ensure that JESJOBS CLASS is set up (Manual) | 366 |
| 8.3.2 Ensure CANCEL JESJOBS profiles are protected (Manual) | 367 |
| 8.3.3 Awareness of the ENCRYPT JESJOBS profiles (Manual) | 369 |
| 8.3.4 Ensure GROUPREG JESJOBS profiles are protected (Manual) | 370 |
| 8.3.5 Ensure HOLD JESJOBS profiles are protected (Manual) | 372 |
| 8.3.6 Ensure JOBCLASS JESJOBS profiles are protected (Manual) | 374 |
| 8.3.7 Ensure JOBNFY JESJOBS profiles are protected (Manual) | 376 |
| 8.3.8 Ensure MODIFY JESJOBS profiles are protected (Manual) | 378 |
| 8.3.9 Ensure PURGE JESJOBS profiles are protected (Manual) | 380 |
| 8.3.10 Ensure RELEASE JESJOBS profiles are protected (Manual) | 382 |
| 8.3.11 Ensure REROUTE JESJOBS profiles are protected (Manual) | 384 |
| 8.3.12 Ensure SPIN JESJOBS profiles are protected (Manual) | 386 |
| 8.3.13 Ensure SPOOLIO JESJOBS profiles are protected (Manual) | 388 |
| 8.3.14 Ensure START JESJOBS profiles are protected (Manual) | 390 |
| 8.3.15 Ensure SUBMIT JESJOBS profiles are protected (Manual) | 392 |
| 8.4 Enable Encryption of Data Set on SPOOL | 394 |
| 8.4.1 Ensure that data sets on SPOOL are encrypted as required (Manual) | 395 |
| 8.4.2 Require user identification (Manual) | 397 |

| | |
|--|------------|
| 8.4.3 Ensure that the JES(BATCHALLRACF) SETROPTS value is set to JES(BATCHALLRACF) (Manual) | 398 |
| 8.4.4 Ensure that the JES(XBMALLRACF) SETROPTS value is set to JES(XBMALLRACF) (Manual) | 399 |
| 8.5 Control Access to Data Sets Used by JES2 | 401 |
| 8.5.1 Ensure that access (read, update and allocate) to the data sets used by JES2 is controlled (Manual) | 402 |
| 8.5.2 Ensure that access to any PROCLIB data sets used by JES2 is protected from unintended updates (Manual) | 404 |
| 8.5.3 Ensure that RACF is called for data sets opened by JES2 (Manual) | 406 |
| 8.6 Device Management | 407 |
| 8.6.1 Ensure that JES2 output devices are controlled (Manual) | 408 |
| 8.6.2 Ensure that bypass label processing (BLP=) is not set on any JOBCLASS (Manual) | 412 |
| 8.6.3 Ensure that use of JES2 input sources are controlled (Manual) | 414 |
| 8.7 JES2 Networking | 416 |
| 8.7.1 Ensure that RJE workstations and NJE nodes are controlled (Manual) | 417 |
| 8.7.2 Ensure that RJE workstations and NJE nodes are controlled (Manual) | 419 |
| 9 UNIX System Services | 421 |
| 9.1 Ensure that z/OS UNIX SURROGAT resources are protected (Automated) | 422 |
| 9.2 Ensure that resources protecting superuser capabilities in the UNIXPRIV class are protected (Automated) | 424 |
| 9.3 Ensure that general users are not allowed to change their file ownership (Automated) | 426 |
| 9.4 Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted (Automated) | 428 |
| 9.5 Ensure that newly assigned UIDs and GIDs are unique values (Automated) | 429 |
| 9.6 Ensure that z/OS UNIX user accounts are defined (Automated) | 431 |
| 9.7 Ensure that RACF Classes required to secure the z/OS UNIX environment are active (Automated) | 433 |
| 9.8 Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTED (Automated) | 435 |
| 9.9 Ensure that the user account for the z/OS UNIX kernel (OMVS) is defined to the security database (Automated) | 437 |
| 9.10 Ensure that z/OS UNIX automount configuration files are protected (Automated) | 439 |
| 9.11 Ensure that z/OS UNIX security parameters in /etc/inetd.conf are configured (Automated) | 441 |
| 9.12 Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured (Automated) | 444 |
| 9.13 Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are set for security (Automated) | 445 |
| 9.14 Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access (Automated) | 447 |
| 9.15 Ensure that BPX resources are protected (Automated) | 449 |
| 9.16 Ensure that security parameters in etc/profile are configured (Automated) | 451 |
| 9.17 Ensure that security commands in /etc/rc are safe (Automated) | 453 |
| 9.18 Ensure that the BPXROOT user account is configured (Manual) | 454 |
| 9.19 Ensure that each RACF group for UNIX is defined with a unique GID (Automated) | 456 |
| 9.20 Ensure that data sets used as step libraries in /etc/steplib are configured (Automated) | 458 |
| 9.21 Ensure that ability to switch into superuser mode is restricted (Automated) | 460 |
| 9.22 Ensure file permission for universal write is restricted (Automated) | 461 |
| 9.23 Ensure USS Telnet server is not active (Automated) | 462 |
| 9.24 Ensure rlogin is not active (Manual) | 463 |
| 9.25 Ensure changes to UNIX file security are logged (Manual) | 464 |
| 9.26 Ensure that programs cannot execute from the /tmp directory (Automated) | 466 |
| 9.27 Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier (Manual) | 469 |
| 9.28 Ensure that daemons are running with z/OS UNIX level security (Automated) | 470 |
| 9.29 Ensure that servers are running with z/OS UNIX level security (Automated) | 472 |

| | |
|--|------------|
| 9.30 Ensure that file systems containing critical data are protected from access using profiles in the FSACCESS class (Manual) | 474 |
| 9.31 Ensure that file systems are mounted read-only wherever possible (Manual) | 476 |
| 9.32 Ensure that file systems are mounted with set-id files disabled wherever possible (Manual) | 478 |
| 9.33 Ensure that no file systems are mounted with security disabled (Automated) | 480 |
| Appendix: Summary Table | 482 |
| Appendix: Change History | 499 |

Overview

All CIS 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 for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

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

This document provides prescriptive guidance for establishing a secure configuration posture for IBM® z/OS® V2R5.

This benchmark assumes that the client is using IBM RACF® as their external security manager (ESM).

This benchmark references the STIGs quite frequently from <https://public.cyber.mil/stigs/>.

Where appropriate, direct reference to the specific STIGs has been documented.

Refer to <https://www.ibm.com/legal/copytrade> for listing of United States trademarks owned by IBM and related information.

UNIX is a registered trademark of The Open Group in the United States and other countries

To obtain the latest version of this guide, please visit <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate IBM z/OS.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention | Meaning |
|--|---|
| <code>Stylized Monospace font</code> | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| <code>Monospace font</code> | Used for inline code, commands, or examples. Text should be interpreted exactly as presented. |
| <i><italic font in brackets></i> | Italic texts set in angle brackets denote a variable requiring substitution for a real value. |
| <i>Italic font</i> | Used to denote the title of a book, article, or other publication. |
| Note | Additional information or caveats |

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.

Impact Statement

Any security, functionality, or operational consequences that can result from following 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.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

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:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor

Shaun Kelley
Barb Leinberger
Mark Nelson
Bruce Wells
Didier Andre
Christopher Meyer
Joe Welsh
Bob Petti
Thomas Wasik

Editor

Anuja Deedwaniya
Eric Pinnell

Recommendations

1 Identification and Authentication

This section provides guidance on how to uniquely identify a user of a system and to prove that a user is genuinely who that person claims to be. It also provides guidance on setting up secure defaults for system and user accounts and their environments.

1.1 Password Control

This section describes the Password Control recommendations.

1.1.1 Ensure that the PASSWORD(INTERVAL) SETROPTS value is set to no longer than 90 days (Automated)

Profile Applicability:

- Level 1

Description:

When a user logs on to the system, RACF compares the system password interval value to the value specified in the user profile. RACF uses the lower of the two values to determine if the user's password has expired.

`PASSWORD (INTERVAL (n))` command sets the maximum age of a password. The `INTERVAL` suboperand specifies the system default for the maximum number "n" of days that each user's password and password phrase remain valid.

If you have the `SPECIAL` attribute, you can specify the `INTERVAL` of the `SETROPTS PASSWORD` command. The `INTERVAL` suboperand specifies the system default for the maximum number of days that each user's password and password phrase remain valid.

Rationale:

The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

To verify a password will expire within 90 days issue the TSO command:

```
SETROPTS LIST
```

and look for the interval value. The `PASSWORD (INTERVAL)` value is found in the return message "PASSWORD CHANGE INTERVAL IS xxx DAYS." xxx will be a value from 1 to 90.

Remediation:

Setting the password interval to 90 days is activated by issuing the TSO command:

```
SETROPTS PASSWORD (INTERVAL (90) )
```

Default Value:

INTERVAL = 30




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223727 Rule ID: SV-223727r604139_rule STIG ID: RACF-ES-000800 Severity: CAT II

Additional Information:

[Health Check: RACF PASSWORD CONTROLS](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. |  |  |  |

1.1.2 Ensure that the `PASSWORD(HISTORY) SETROPTS` value is set to at least 4 (Automated)

Profile Applicability:

- Level 1

Description:

`HISTORY` specifies the number of previous passwords that RACF saves for each user ID and compares with an intended new password. If there is a match with one of the previous passwords, or with the current password, RACF rejects the intended new password. Set the `PASSWORD(HISTORY(n))` RACF option “n” value to 4 or more.

`PASSWORD(HISTORY(n))` command enables you to specify the number of previous passwords and password phrases (1 - 32) that RACF saves for each user and compares it with an intended new value. For passwords, RACF stores only previous passwords in each user's history. For password phrases, RACF saves the user's current password phrase in addition to the user's previous password phrases. Therefore, for password phrases, RACF saves one fewer previous value than the number you specify for history.

Example: If you specify 12 for your `HISTORY` number using the command `SETROPTS PASSWORD(HISTORY(12))` RACF saves up to 12 previous passwords and up to 11 previous password phrases for each user. Effective immediately, the values when executing that command are the default values for new users whom you define to RACF® through the `ADDUSER` command.

Rationale:

Not setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

To verify a password history will have 4 or more generations issue the TSO command:

```
SETROPTS LIST
```

and look for the history value “x” in the `PASSWORD(HISTORY)` return message “x GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.” x will be greater than or equal to 4.

Remediation:

Setting the password history to 4 generations is activated by issuing the TSO command:

```
SETROPTS PASSWORD(HISTORY(4))
```




Default Value:

NOHISTORY

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223728 Rule ID: SV-223728r604139_rule STIG ID: RACF-ES-000810 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|--|--|--|
| v8 | 5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |

1.1.3 Ensure that the PASSWORD(RULEn) SETROPTS value(s) is set (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(RULEn(LENGTH(m1:m2) content-keyword(position))) specifies an individual syntax rule for new passwords that users create at logon, on JCL jobcards, or on the PASSWORD command and for passwords specified on ALTUSER commands that have the NOEXPIRED operand. Eight syntax rules are allowed. Therefore, for the RULEn suboperand, the value of n is 1 - 8.

At a minimum require at least 8 characters with a mix of character types.

Rationale:

The rule value(s) specify the rules that RACF will apply when a user selects a new password. Improper setting of any of these fields, individually or in combination with another, can result in weakened passwords and compromise the security of the processing environment.

Audit:

To verify password syntax rules issue the TSO command:

```
SETROPT LIST
```

Rules in effect are found under the "INSTALLATION PASSWORD SYNTAX RULES:" message. Verify at least one password rule under "INSTALLATION PASSWORD SYNTAX RULES" is defined with the values shown below:

```
LENGTH(8) xxxxxxxx
```

Remediation:

Setting the password syntax to require a length of 8 and a mix of character types is activated by issuing the TSO command:

```
SETROPTS PASSWORD(RULE1(LENGTH(8) MIXEDALL(1:8))
```

Default Value:

NORULES




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223724 Rule ID: SV-223724r604139_rule STIG ID: RACF-ES-000770 Severity: CAT II

Additional Information:

[Health Check: RACF PASSWORD CONTROLS](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |

1.1.4 Ensure that the SETROPTS PASSWORD(MINCHANGE(n)) value will specified a value greater the zero (0) (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS PASSWORD(MINCHANGE(nnn)) specifies the number of days that must pass between a user's password and password phrase changes. Users can not change their own passwords and password phrases within the minimum change interval. Permitting users to change their password more than once in a day allows users to quickly cycle through their password history and maintain the same password indefinitely. The SETROPTS PASSWORD(MINCHANGE(nnn)) value, either specified or defaulted, is in effect for all users. A security administrator may set a password within the MINCHANGE window.

Rationale:

The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment.

Audit:

Verify the MINCHANGE value by issuing the TSO command:

```
SETROPTS LIST
```

Look for the following message "PASSWORD MINIMUM CHANGE INTERVAL IS x DAYS." x will be a value from 1 to 254.

Remediation:

Issue the TSO command:

```
SETROPTS PASSWORD(MINCHANGE(1))
```




Default Value:

The initial default is 0 days, allowing users to change their passwords and password phrases more than once on the same day.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223726 Rule ID: SV-223726r604139_rule STIG ID: RACF-ES-000790 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |

1.1.5 Ensure that the PASSWORD(REVOKE) SETROPTS value is specified (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS PASSWORD(REVOKE(nnn))` enables you to specify how many consecutive incorrect password and password phrase attempts RACF permits before it revokes the user ID on the next attempt. If you specify a `REVOKE SETROPTS` value, ensure `INITSTATS` are in effect.

If `SETROPTS NOREVOKE` is in effect, consecutive incorrect passwords and password phrases are ignored.

Rationale:

The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment.

Audit:

Issue TSO command:

```
SETROPTS LIST
```

Look for the following message: "AFTER x CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID WILL BE REVOKED"

Remediation:

Issue TSO command:

```
SETROPTS PASSWORD(REVOKE(6))
```

Default Value:

The default value is `SETROPTS PASSWORD(NOREVOKE)`.

Note that `SETROPTS PASSWORD(REVOKE(nnn))` requires that `SETROPTS INITSTATS` has been enabled.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223695 Rule ID: SV-223695r604139_rule STIG ID: RACF-ES-000480 Severity: CAT II
2. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223696 Rule ID: SV-223696r604139_rule STIG ID: RACF-ES-000490 Severity: CAT II

Additional Information:

[Health Check: RACF PASSWORD CONTROLS](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.3 Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. |  |  |  |

1.1.6 Ensure that the KDFAES algorithm is used to protect passwords in the security database (Automated)

Profile Applicability:

- Level 2

Description:

By default passwords stored in RACF are protected using a weak DES based algorithm. Using off the shelf applications and hardware, it is a relatively simple operation to reverse engineer the encryption key – RACF user ID's password – or perform a brute-force offline attack. Any user with access to RACF database may obtain the passwords for all user IDs in the system.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Check `SETROPTS LIST` output for the current password processing options. Look for the use of a `LEGACY` password encryption algorithm.

The TSO command that is to be issued by an RACF authorized user is:

| |
|----------------------------|
| <code>SETROPTS LIST</code> |
|----------------------------|

Look for the following message "PASSWORD PROCESSING OPTIONS: THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES"

Remediation:

KDFAES is enabled using the `SETROPTS` command exit:

```
SETROPTS PASSWORD (ALGORITHM (KDFAES) )
```

When `KDFAES` is enabled, existing DES passwords will continue to be evaluated by RACF. User passwords do not need to be changed. When the user next changes his password, it will be encrypted using the `KDFAES` algorithm. The `PWCONVERT` operand of the `ALTUSER` command can be used to transform a `DES` password (but not a password phrase) into a `KDFAES` password without requiring the password to be changed.

```
ALTUSER <user-id> PWCONVERT
```

The installation can create a command list (`CLIST`) which converts the passwords of all users with the RACF `SEARCH` by issuing the TSO command:

```
SEARCH CLASS (USER) CLIST ('ALTUSER ' ' PWCONVERT')
```

The command list that is created is placed in the data set `<user-id>.EXEC.RACF.CLIST`. It will contain `ALTUSER` commands for user IDs which don't have passwords, such as `PROTECTED` users and anchor user IDs like `irrcerta`, `irrmulti`, and `irrcerto`.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223729 Rule ID: SV-223729r604139_rule STIG ID: RACF-ES-000820 Severity: CAT I

Additional Information:

[Health Check: RACF ENCRYPTION ALGORITHM](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. | | ● | ● |

1.1.7 Ensure that the PASSWORD(WARNING) SETROPTS value is set (Automated)

Profile Applicability:

- Level 1

Description:

`WARNING` specifies the number of days before a password expires when RACF is to issue a warning message to the user.

Rationale:

System users should be warned about impending password expiration to allow secure passwords to be chosen and to allow the changing of a password at a convenient time to help minimize password change impact.

Audit:

Issue TSO command:

```
SETROPTS LIST
```

Look for the following message: `PASSWORD(WARNING)` value shows "PASSWORD EXPIRATION WARNING LEVEL IS xxx DAYS."

Remediation:

It is a common industry practice to notify users that a password change will be required in no less than 5 days. This time interval may be increased but should not be less than 5 days. `WARNING` is activated with the command:

```
SETR PASSWORD(WARNING(5))
```

Default Value:

`SETROPTS PASSWORD(NOWARNING)` is the default.

Note that `SETROPTS PASSWORD(WARNING(nnn))` requires that `SETROPTS INITSTATS` has been enabled.

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V-275

1.2 System Settings

This section describes the System Settings recommendations.

1.2.1 Ensure that Inactive users are revoked (Automated)

Profile Applicability:

- Level 1

Description:

`PASSWORD (INACTIVE (nnn))` command specifies the number of days (1 - 255) that a user ID can remain unused and still be considered valid. RACF user verification checks the number of days since the last successful time the user accessed the system against the `INACTIVE` value and, if the former is larger, revokes the user's right to use the system.

`INACTIVE` does not apply to Protected user IDs. Protected user IDs are protected from being revoked through inactivity. If you specify `INACTIVE`, `INITSTATS` must be in effect. If the backup database is needed but does not contain current information, some user IDs can be revoked because they appear to have been unused beyond the number of days specified on the `INACTIVE` operand.

`NOINACTIVE` specifies that RACF user verification is not to check user IDs against an unused-userid-interval.

Inactive user IDs are to be revoked after a period of inactivity not to exceed 90 days.

Rationale:

Inactive user IDs are vulnerable to attack because no one is watching these IDs. A password change request might go unnoticed for a user that has not accessed the system for several months. Actively resuming an expired user ID brings attention to that ID.

Audit:

Issue TSO command:

```
SETROPTS LIST
```

Look for the following message:

"INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER xxx DAYS"

or

"INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED."

Remediation:

Issue TSO command:

```
SETROPTS PASSWORD (INACTIVE (90) )
```




Default Value:

`NOINACTIVE`

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223723 Rule ID: SV-223723r604139_rule STIG ID: RACF-ES-000760 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 5.3 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. |  |  |  |

1.2.2 Ensure that *STARTED* class is used to assign users to Started Tasks (Automated)

Profile Applicability:

- Level 1

Description:

Started procedures have system generated job statements that do not contain the user, group, or password statements. To enable the started procedure to access the same protected resources that users and groups access, started procedures must have an associated user ID. If a user ID is not associated with the started procedure, the started procedure will not have access to the resources.

User ID can be assigned through the `STARTED` class or through the `ICHRIN03` table. As it is easily auditable, does not require assembler knowledge or system `IPL` we would recommend the usage of the `STARTED` class.

Rationale:

If a user ID is not associated with the started procedure, the started procedure will not have access to the resources.

Audit:

To verify if a started procedure is associated with a user ID the `STARTED` class profile and its `STDATA` segment can be listed, the `USER=` parameter in the `STDATA` segment will be the associated user.

```
RLIST STARTED procedure.* STDATA
```

Remediation:



Default user should not be usable.

```
RDEFINE STARTED procedure.*  
RALTER STARTED procedure.* STDATA(USER(userid))
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223719 Rule ID: SV-223719r604139_rule STIG ID: RACF-ES-000720 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|---|---|
| v8 | 5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | |  |  |

1.2.3 Ensure user propagation is protected with the PROPCNTL class (Automated)

Profile Applicability:

- Level 1

Description:

Batch jobs that are user-submitted to the operating system should inherit the user ID of the submitter. This will identify the batch job with the user for the purpose of accessing resources. In some environments, such as CICS jobs submitted without the USER operand specified on the JOB statement run under a user ID other than the user submitting the job, in this case, the CICS user ID. This situation presents a security violation in that the issuer of the job will inherit the authority of the CICS user ID. The PROPCNTL Class was designed to prevent this from occurring. Utilize propagation control (PROPCNTL) for system-level address spaces that submit jobs on behalf of users.

Rationale:

Jobs submitted without the USER operand specified on the JOB statement run under a user ID other than the user submitting the job presents a security violation in that the issuer of the job will inherit the authority of the user ID.

Audit:

Verify that the PROPCNTL class is active and the user ID that should not be propagated

```
SETROPTS LIST
RLIST PROPCNTL userid
```

Remediation:




Activate the PROPCNTL class and define the users that should not be propagated

```
SETROPTS CLASSACT(PROPCNTL)
SETROPTS RACLIST(PROPCNTL)
RDEFINE PROPCNTL userid
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223673 Rule ID: SV-223673r604139_rule STIG ID: RACF-ES-000250 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

1.2.4 Ensure that Job wait time option is set (Automated)

Profile Applicability:

- Level 1

Description:

In `SMFPRMxx` the `JWT (n)` parameter specifies the maximum amount of consecutive time that an executing job may spend as ineligible to use any CPU resources before being canceled for inactivity.

Rationale:

Address spaces of inactive users must be terminated after a short period of time to limit risk of session stealing. `JWT(0015)` is suggested so users inactive for 15 minutes are terminated.

Audit:

The z/OS console command `DISPLAY SMF` can be used to check for the current active options.

```
D SMF,0
```




Remediation:

The parameter `JWT(0015)` must be coded in the `SMFPRMxx` member of `parmlib`.

Default Value:

`JWT(0010)`

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

1.2.5 Ensure that started tasks defined with the trusted attribute are justified (Manual)

Profile Applicability:

- Level 1

Description:

Trusted Started tasks bypass RACF checking. It is vital that this attribute is NOT granted to unauthorized Started Tasks which could then obtain unauthorized access to the system.

Rationale:

Unauthorized Started Tasks obtaining unauthorized access to the system could result in the compromise of the confidentiality, integrity, and availability of the operating system, RACF, or customer data.

Audit:

To verify the `TRUSTED` attribute, issue the command:

```
RLIST STARTED startedtask.** STDATA
```

Remediation:

The trusted attribute can be removed with the following command:

```
ralter STARTED startedtask.** STDATA (NOTRUSTED)
```

Default Value:

NOTRUSTED

References:




1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223661 Rule ID: SV-223661r604139_rule STIG ID: RACF-ES-000130 Severity: CAT II

Additional Information:

[IBM publishes a list of the z/OS started tasks where the Trusted attribute is recommended.](#)

For other software, consult the vendor for recommendations.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |

1.2.6 Ensure that the OPERCMDS resource class is ACTIVE and RACLISed (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS CLASSACT (OPERCMDs)` specifies that the class `OPERCMDs` will have RACF protection is to be in effect for it.

These values become effective immediately after the command `SETROPTS CLASSACT (OPERCMDs)` is issued.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. Failure to define access to z/OS system commands could result in unauthorized personnel issuing sensitive system commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Issue the `SETROPTS LIST` command and look for the `OPERCMDs` class in 'ACTIVE CLASSES =' section and that the class is also listed as `RACLISed`.

```
SETROPTS LIST
```

Verify the list of commands protected by the `OPERCMDs` class

```
SR CLASS (OPERCMDs)
```

For each profile, verify that the definitions are as expected.

```
RLIST OPERCMDs profile.from.opercmds
```

Remediation:

Activate and `RACLIS` the `OPERCMDs` class.

Issue the command:

```
SETROPTS CLASSACT (OPERCMDs) RACLIS (OPERCMDs)
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223658 Rule ID: SV-223658r604139_rule STIG ID: RACF-ES-000100 Severity: CAT II




Additional Information:

[Health Check: RACF OPERCMDS ACTIVE](#)

[z/OS Security Server RACF Security Administrator's guide:](#)

[z/OS Planning for Multilevel Security and the Common Criteria:](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

1.2.7 Ensure that CONSOLE resource class is ACTIVE (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

Rationale:

Failure to control access to MCS consoles reduces the exposure that threatens the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

Audit:

Issue the `SETROPTS LIST` command and verify that the `CONSOLE` class is in the list of active classes.

```
SETROPTS LIST
```

Remediation:

Issue the `SETROPTS` command to activate and `RACLIST` the `CONSOLE` class with this command:

```
SETROPTS CLASSACT(CONSOLE) RACLIST(CONSOLE)
```




Default Value:

The `CONSOLE` class is inactive.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223659 Rule ID: SV-223659r604139_rule STIG ID: RACF-ES-000110 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

1.2.8 Ensure that FACILITY resource class is ACTIVE and RACLISTED (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS CLASSACT(FACILITY) specifies that the class FACILITY class is active and that RACF protection is to be in effect for it.

These values become effective immediately after the command SETROPTS CLASSACT(FACILITY) and SETROPTS RACLIST(FACILITY) are issued.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the command:

```
SETROPTS LIST
```

Look for the FACILITY class in 'ACTIVE CLASSES =' section.

Remediation:

Issue the command:

```
SETROPTS CLASSACT(FACILITY) RACLIST(FACILITY)
```

Default Value:

The FACILITY class is inactive.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223657 Rule ID: SV-223657r604139_rule STIG ID: RACF-ES-000090 Severity: CAT II

Additional Information:

[Health Check: RACF FACILITY ACTIVE](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

1.2.9 Ensure that inapplicable PPT entries have been invalidated (Manual)

Profile Applicability:

- Level 1

Description:

The program properties table (PPT) contains entries for special attributes of programs. One of these entries indicates whether or not the program is allowed to bypass datasets password protection (PPTNOPAS), or access key protected storage.

Rationale:

If invalid or inapplicable PPT entries exist, a venue is provided for the introduction of trojan horse modules with security bypass capabilities.

Audit:

The recommended attributes for the modules must be compared with the vendor recommended attributes to list the PPT modules and their current attributes, you can use the following z/OS console command:

```
D PPT
```

Remediation:

The attributes must be set accordingly to the vendor recommendation in the SCHEDxx parmlib member.

Review the modifications with the following z/OS command:

```
SET SCH=XX
```




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223785 Rule ID: SV-223785r604139_rule STIG ID: RACF-OS-000290 Severity: CAT I

Additional Information:

[IBM publish the list of modules and their recommend attributes with each release of z/OS. For z/OS 2.5.](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |

1.2.10 Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) currently active parmlib data set(s) (Automated)

Profile Applicability:

- Level 1

Description:

Specifying `LNKAUTH=APFTAB` in the `IEASYSxx` member(s) currently active `parmlib` data set(s) allows libraries other than those designated as `APF` to contain authorized modules by adding to this list all libraries in the `LNKLST` concatenation when accessed as part of the linklist concatenation.

Rationale:

Failure to specify `LNKAUTH=APFTAB` allows libraries other than those designated as `APF` to contain authorized modules which could bypass security and violate the integrity of the operating system environment. This expanded authorization list inhibits the ability to control exclusion of unauthorized modules.

Audit:

Check the current `IEASYSxx` parameters and look for the `LNKAUTH` parameter. If `LNKAUTH=LNKLST` is found (or not specified), it should be remediated.

| |
|----------------|
| D PROG, LNKLST |
|----------------|

Remediation:

Change `LNKAUTH=LNKLST` to `LNKAUTH=APFTAB` and re-ipl the system when possible.




Default Value:

`LNKAUTH=LNKLST`

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223786 Rule ID: SV-223786r604139_rule STIG ID: RACF-OS-000300 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

1.2.11 Ensure that the CONSOLxx members are configured (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

Audit:

Check each `CONSOLxx parmlib` member for the following.

The `DEFAULT` statement for each `CONSOLxx` member specifies `LOGON (REQUIRED)` or `LOGON (AUTO)`.

- The `CONSOLE` statement for each console assigns a unique name using the `NAME` parameter.
- The `CONSOLE` statement for each console specifies `AUTH (INFO)`. Exceptions are the `AUTH` parameter is not valid for consoles defined with `UNIT (PRT)` and specifying `AUTH (MASTER)` is permissible for the system console.

Note: The site should be able to determine the system consoles. However, it is imperative that the site adhere to the `DEFAULT` statement requirement.

Remediation:

Ensure that the `DEFAULT` statement specifies `LOGON (REQUIRED)` so that all operators are required to log on prior to entering z/OS system commands. At the discretion of the ISSO, `LOGON (AUTO)` may be used. If `LOGON (AUTO)` is used assure that the console user IDs are defined with minimal access.




Ensure that each `CONSOLE` statement specifies an explicit console `NAME` and that `AUTH (INFO)` is specified, this also including extended MCS consoles. `AUTH (MASTER)` may be specified for systems console.

Note: The site should be able to determine the system consoles. However, it is imperative that the site adhere to the `DEFAULT` statement requirement.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223715 Rule ID: SV-223715r604139_rule STIG ID: RACF-ES-000680 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

1.2.12 Ensure that no expired digital certificates are used (Automated)

Profile Applicability:

- Level 1

Description:

The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a relying Party that the unique binding is secure.

Rationale:

Audit:

Check the expiration (End Date) for each certificate with a status of `TRUST`

| |
|------------------------|
| RACDCERT CERTAUTH LIST |
|------------------------|




Remediation:

If the certificate is a user or device certificate with a status of `TRUST` follow procedures to obtain a new certificate or re-key certificate. If it is an expired `CA` certificate remove it. NOTE: Certificates used for password enveloping can continue to be used after expiring, and it should not be removed if password enveloping is still active.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223647 Rule ID: SV-223647r604139_rule STIG ID: RACF-CE-000020 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. |  |  |  |

1.2.13 Ensure that RACF RVARYPW are set to non-default values (Automated)

Profile Applicability:

- Level 1

Description:

The `SETROPTS RVARYPW([SWITCH(switch-pw)][STATUS(status-pw)])` command specifies the passwords that the operator is to use to respond to requests to approve `RVARY` command processing, where `switch-pw` is the response to a request to switch RACF databases or change the operating mode of RACF, and `status-pw` is the response to a request to change RACF or database status from `ACTIVE` to `INACTIVE` or from `INACTIVE` to `ACTIVE`. Different passwords can be specified for each response.

Note that `NO` is not a valid password for either `SWITCH` or `STATUS`.

These values become effective immediately when RACF is activated for the first time.

Rationale:

Failure to change the documented default values will allow any general user to change the status of the RACF database.

Audit:

Issue the command:

```
SETROPTS LIST
```

The state of the `RVARY` `SWITCH` and `STATUS` passwords are displayed:

- INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
- INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.

Remediation:

Issue the command:

```
RVARYPW([SWITCH(switch-pw)][STATUS(status-pw)])
```




Default Value:

When RACF is using a newly initialized database, the switch password and the status password are both set to `YES`.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223702 Rule ID: SV-223702r604139_rule STIG ID: RACF-ES-000550 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. |  |  |  |

1.3 User Attributes

This section describes the User Attributes recommendations.

1.3.1 Ensure that the use of RACF SPECIAL Attribute is justified (Manual)

Profile Applicability:

- Level 1

Description:

The SPECIAL user attribute allows full authorization to modify all profiles in RACF database and allows the user to perform all RACF functions, except those requiring AUDITOR or ROAUDIT attributes. The Group-Special attribute allows decentralized RACF control of datasets and resources. In cases where the scope of authority granted to a Group-Special Administrator has an impact on system security, the installation needs to be fully aware and approve its use. This privilege should be limited to the security group and administrators because of the extreme control that these users have.

Rationale:

Users with SPECIAL privilege can alter any profile and give themselves permissions to alter data, including logging and audit data.

Audit:

Find all the user IDs who have the SPECIAL attribute and validate the need for the user to have the privilege.

Execute the RACF Data Security Monitor Utility (ICHDSM00).

Examine the Selected User Attribute Report:

```
//ICHDSM00 JOB CLASS=A,NOTIFY=&SYSUID,MSGCLASS=H  /*-----  
-----  
//ICHDSM00 EXEC PGM=ICHDSM00  
//SYSPRINT DD SYSOUT=*  
//SYSUT2 DD SYSOUT=*  
//SYSIN DD DUMMY
```

Remediation:

Use the ALTUSER command or the CONNECT command to remove the attribute from the user.




Default Value:

The SPECIAL attribute is assigned by default only to the user IBMUSER. This user ID should be revoked immediately after RACF has been installed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223713 Rule ID: SV-223713r604139_rule STIG ID: RACF-ES-000660 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |

1.3.2 Ensure that SYS1.UADS contains only emergency use user IDs (Manual)

Profile Applicability:

- Level 1

Description:

SYS1.UADS is a dataset where LOGONIDs will be maintained with applicable password information when RACF is not functional.

Rationale:

If an unauthorized user has access to SYS1.UADS they could enter their LOGONID and password into the SYS1.UADS dataset and could give themselves access to the system.

Audit:

SYS1.UADS is defined but only contains firecall user IDs. Firecall IDs are those that are SPECIAL level users but are only to be activated during emergencies when RACF database is unavailable.

Remediation:

Move all non-emergency user IDs into RACF. Delete all non-emergency user IDs from SYS1.UADS.




Default Value:

SYS1.UADS has no user IDs defined.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223837 Rule ID: SV-223837r604139_rule STIG ID: RACF-TS-000020 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. |  |  |  |

1.3.3 Ensure that MCS console user ID(s) is protected (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. When using the `LOGON(AUTO)` control, a user with the name of the MCS console will be used for access checking.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands.

Audit:

For each of the console names found in `CONSOLxx`, verify that:

- The user has been defined in RACF
- The user has no RACF privileges (`SPECIAL`, `OPERATIONS`, ...)
- The user can't use online facilities (`TSO`, `CICS`, ...)
- The user is only permitted to the resources in `MVS.MCSOPER.consolename` in the `OPERCMD` class and defined in the `CONSOLE` class.
The `IRRUT100` utility can be used to check all the authorizations of the user(s).
Issue the command:

```
IRRUT100 EXEC PGM=IRRUT100
//IRRUT100 EXEC PGM=IRRUT100
//SYSUT1 DD UNIT=SYSDA,SPACE=(TRK,(5,1))
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
consolename
/END
```

Remediation:

If any resource or dataset is permitted to the console user (or group) they must be removed.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223716 Rule ID: SV-223716r604139_rule STIG ID: RACF-ES-000690 Severity: CAT II

Additional Information:

[IRRUT100 example](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

1.3.4 Ensure that all STARTED class profiles specify PROTECTED user IDs (Automated)

Profile Applicability:

- Level 1

Description:

Started procedures have system generated job statements that do not contain the user, group, or password statements.

Rationale:

If a user ID is not associated with the started procedure, the started procedure will not have access to the resources. If a started procedure is associated with an incorrect user or a user with higher than necessary authority, then a potential vulnerability exists.

Audit:

Verify that the users associated with started tasks have the PROTECTED attribute. List each started profile to obtain its user ID then list that user by issuing the commands:

```
SEARCH CLASS(STARTED)
RLIST STARTED <profile-name> STDATA NORACF

STDATA INFORMATION
-----
USER= <userid>
GROUP=
TRUSTED= YES
PRIVILEGED= NO
TRACE= NO

LISTUSER <userid>

ATTRIBUTES=PROTECTED
```

Look for ATTRIBUTES=PROTECTED.

Remediation:




If the user is not PROTECTED, remove the password/passphrase attributes to make it PROTECTED with this command:

```
CALTUSER userid NOPASSWORD NOPHRASE
```


References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223719 Rule ID: SV-223719r604139_rule STIG ID: RACF-ES-000720 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2 Authorization and Access Control Management

This section provides guidance on how to ensure that users only have access to the system resources necessary for their role.

Authorization is dependent on identification and authentication.

2.1 Data Protection

2.1.1 Ensure that Maintenance user IDs are protected (Manual)

Profile Applicability:

- Level 1

Description:

DASD management user ID require access to backup and restore all files and present a high degree of risk to the environment.

Users are given access to perform necessary functions thru use of the `DASDVOL` class (for `non-SMS` volumes) and/or thru `STGADMIN` profiles in the `FACILITY` class for `SMS` managed volumes. Access to individual profiles in the `DATASET` class should be disallowed.

Rationale:

Failure to maintain user id access reduces the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

Audit:

`DASDVOL` and `STGADMIN` profiles are restricted to storage management personnel only.

Remediation:

Ensure that `DASDVOL` and `STGADMIN` profiles reflect the needs of storage management personnel. Non-storage management personnel should not have this access.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223732 Rule ID: SV-223732r604139_rule STIG ID: RACF-ES-000850 Severity: CAT II

Additional Information:

- [OPERATIONS and DASDVOL authority](#)
- [Storage Administration \(STGADMIN\) Profiles in the FACILITY Class or XFACILIT Class](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.2 Ensure that access to active SMF collection files is controlled (Automated)

Profile Applicability:

- Level 1

Description:

SMF data collection is the system activity journaling facility of the z/OS system. With the proper parameter designations, it serves as the basis to ensure individual user accountability. `SYS1.MANxx` datasets should be created once and reused when cleared.

Update and allocate access to SMF collection files (i.e., `SYS1.MANx`, `logger`) are limited to system programmers and/or batch jobs that perform SMF dump processing. Control access based on type - separate collection as much as possible.

Rationale:

Users may have `UPDATE` access to the datasets, but `ALTER` allows for dataset deletion and should be avoided. `ALTER` access reduces the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

Audit:

All entities on the `ACL` for `SYS1.MANxx` datasets are no higher than `UPDATE`.

Remediation:

Change dataset access from `ALTER` to `UPDATE` for users and groups on the `ACL`.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223701 Rule ID: SV-223701r604139_rule STIG ID: RACF-ES-000540 Severity: CAT II

2.1.3 Ensure that the *WHEN(PROGRAM) SETROPTS* value is active (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS WHEN (PROGRAM)` activates RACF program control, which includes both access control to load modules and program access to data sets.

To set up access control to load modules, you must identify your controlled programs by creating a profile for each in the `PROGRAM` class. To set up program access to data sets, you must add a conditional access list to the profile of each program-accessed data set. Then, when program control is active, RACF ensures that each controlled load module is executed only by callers with the defined authority. RACF also ensures that each program-accessed data set is opened only by users who are listed in the conditional access list with the proper authority and who are executing the program specified in the conditional access list entry.

Ensure that RACF will perform program control.

Rationale:

Not protecting critical programs and not ensuring a clean address space can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the command:

```
SETROPTS LIST
```

Then look for `WHEN (PROGRAM)` in the `ATTRIBUTES =` section.

Example:

```
ATTRIBUTES = INITSTATS WHEN (PROGRAM -- BASIC)
```

Remediation:

Issue the command:

```
SETROPTS WHEN (PROGRAM)
```

Default Value:

`NOWHEN(PROGRAM)`

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223708 Rule ID: SV-223708r604139_rule STIG ID: RACF-ES-000610 Severity: CAT II

Additional Information:

[Protecting programs](#)

2.1.4 Ensure that the ICHDSM00 program is protected (Automated)

Profile Applicability:

- Level 1

Description:

ICHDSM00 is the data security monitor utility. READ authority to this program in the PROGRAM class is one way a user can have authority to run the utility. RACF ships the utility in SYS1.LINKLIB. Further, SYS1.LINKLIB is generally one of the code libraries identified in the PROGRAM * or ** profile and is always treated as UACC(READ) , even if the profile itself has a more restrictive UACC.

Therefore, a more specific PROGRAM profile should be defined to protect ICHDSM00.

Rationale:

ICHDSM00 provides information on the security posture of the system. Such information should not be available to general users.

Audit:

To see if ICHDSM00 is explicitly protected issue the command:

```
RLIST PROGRAM ICHDSM00 ALL
```

Remediation:

Define a PROGRAM profile named ICHDSM00 with the following attributes:

- UACC(NONE)
- No ID(*) on the access list
- READ access is restricted to system programmers and/or security personnel with a need to know, who do not already have the AUDITOR or ROAUDIT attributes
- All accesses are being logged




Default Value:

ICHDSM00 is not explicitly protected in the PROGRAM class.

Additional Information:

1. The instructions for protecting ICHDSM00 are documented in the following section of the RACF Security Administrator's Guide:
 - [Maintaining a clean environment in BASIC or ENHANCED mode](#)
2. The data security monitor utility is documented in the RACF Auditor's Guide:
 - [The data security monitor \(DSMON\)](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.5 Ensure that the IRRDPI00 program is protected (Automated)

Profile Applicability:

- Level 1

Description:

ICHDPI00 is the program that is used to update the dynamic parse function in RACF, and to refresh in-storage custom field data after making updates in the CFIELD class. READ authority to this program in the PROGRAM class is one way a user can have authority to run the program. RACF ships the program in SYS1.LINKLIB. Further, SYS1.LINKLIB is generally one of the code libraries identified in the PROGRAM * or ** profile, and is always treated as UACC(READ). even if the profile itself has a more restrictive UACC.

Therefore, a more specific PROGRAM profile should be defined to protect IRRDPI00.

Rationale:

IRRDPI00 updates the RACF configuration, and thus access should not be allowed for general users.

Audit:

To see if IRRDPI00 is explicitly protected issue the command:

```
RLIST PROGRAM IRRDPI00 ALL
```

Remediation:

1. Define a PROGRAM profile named IRRDPI00 with the following attributes:
 - UACC(NONE)
 - No ID(*) on the access list
2. If you have non-SPECIAL users with a need to issue the IRRDPI00 command, use the IRRDPI00 profile in the FACILITY class to grant access. This profile should have the following attributes:
 - UACC(NONE)
 - No ID(*) on the access list
 - Not in WARNING mode
 - READ access is restricted to system programmers and security personnel with a need to use the IRRDPI00 command
 - All accesses are being logged




Default Value:

ICHDPM00 is not explicitly protected in the PROGRAM class.

Additional Information:

1. The instructions for protecting IRRDPI00 are documented in the following section of the RACF Security Administrator's Guide:
 - o [Maintaining a clean environment in BASIC or ENHANCED mode](#)
2. Authorization requirements for IRRDPI00 are documented in the RACF System Programmer's Guide:
 - o [RACF authorization of the IRRDPI00 command](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.6 Ensure that the SETROPTS ERASE value is set to ERASE(ALL) on all systems (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS ERASE(ALL) specifies that data management is to erase all scratched data sets including temporary data sets. NOERASE specifies that no DASD data sets are erased when deleted.

The system-wide options control the default settings for determining how RACF will function when handling requests for access to the operating system environment, RACF, and customer data. RACF provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used.

Rationale:

Not maintaining these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Impact:

The impact of SETROPTS ERASE(ALL) is directly proportional to the amount of DASD space which is being deleted. While recent releases of z/OS have substantially improved the performance of data set erasure, there may be system impacts if a large amount of DASD space is being erase.

Audit:

Issue command:

```
SETROPTS LIST
```

Set ERASE values as follows:

```
ERASE-ON-SCRATCH IS ACTIVE, CURRENT OPTIONS:  
ERASE-ON-SCRATCH FOR ALL DATA SETS IS IN EFFECT
```

Remediation:

To show the status of RACF Controls including the status of the ERASE options issue Command:

```
SETR LIST
```

To enable Erase On Scratch for all datasets issue the command:

```
SETR ERASE (ALL)
```

Default Value:

SETROPTS NOERASE

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223731 Rule ID: SV-223731r604139_rule STIG ID: RACF-ES-000840 Severity: CAT II

Additional Information:

1. [See the section titled “Erasing Scratched or Released Data” in the RACF Security Administrator’s Guide](#)
2. [Health Check RACF ERASE ON SCRATCH](#)

2.1.7 Ensure that the TEMPDSN class is active (Automated)

Profile Applicability:

- Level 1

Description:

SETROPTS CLASSACT(TEMPDSN) provides protection for DFP-managed temporary data sets if these data sets are not deleted by the job or session which created them.

Rationale:

You can protect DFP-managed temporary data sets. Normally, these data sets are considered protected from any accesses except by the job or session that created them, and therefore do not need to be protected by RACF®. However, the following situations could leave a temporary data set unprotected:

- A system failure
- An initiator failure or initiator termination by the FORCE command
- An automatic restart - between the failure and the restart

In these cases, if the TEMPDSN class is active, only users with the OPERATIONS attribute can scratch any residual DFP-managed temporary data sets remaining on a volume.

Audit:

Look for the TEMPDSN class in ACTIVE CLASSES = section after issuing the command:

```
SETROPTS LIST
```

Remediation:

Issue the command:

```
SETROPTS CLASSACT(TEMPDSN)
```

Default Value:

SETROPTS NOCLASSACT(TEMPDSN)

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223660 Rule ID: SV-223660r604139_rule STIG ID: RACF-ES-000120 Severity: CAT II

Additional Information:

[Health Check RACF TEMPDSN ACTIVE](#)

[Protecting temporary data sets” in the RACF Security Administrator’s Guide](#)

2.1.8 Ensure the RACF security data sets and all copies are protected (Automated)

Profile Applicability:

- Level 1

Description:

RACF database files contain all access control information for the operating system environment and system resources as well as user registry, user permissions and user authentication data.

RACF data set rules for RACF security data sets and/or databases restrict READ access to auditors and processes which perform RACF database backup operations.

RACF data set rules for RACF security data sets and/or databases restrict READ and/or greater access to z/OS systems programming personnel, security personnel, and/or batch jobs that perform RACF maintenance.

All (i.e., failures and successes) data set access authorities (i.e. `READ`, `UPDATE`, `ALTER`, and `CONTROL` for RACF security data sets and/or databases are logged."

Note: Active and backup datasets, that may be split across multiple datasets, or any offloaded copy must be protected.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

- RACF data set rules for RACF security data sets and/or databases restrict READ access to auditors and processes which perform RACF database backup operations.
- RACF data set rules for RACF security data sets and/or databases restrict READ and/or greater access to z/OS systems programming personnel, security personnel, and/or batch jobs that perform RACF maintenance.
- All (i.e., failures and successes) data set access authorities (i.e. `READ`, `UPDATE`, `ALTER`, and `CONTROL`) for RACF security data sets and/or databases are logged.

Remediation:

Review access authorization to critical security database files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect RACF Files.

Ensure that `READ` and/or greater access to all RACF files and/or databases are limited to system programmers and/or security personnel, and/or batch jobs that perform RACF maintenance. `READ` access can be given to auditors and DASD batch. All accesses to RACF files and/or databases are logged.

Default Value:

`SETROPTS PROTECTALL` controls the default access allowed for data sets.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223685 Rule ID: SV-223685r604139_rule STIG ID: RACF-ES-000370 Severity: CAT I

Additional Information:

[Health Check RACF SENSITIVE RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.9 Ensure the RACF remote sharing facility files are protected (Automated)

Profile Applicability:

- Level 1

Description:

When using the RACF remote sharing facility (`RRSF`) to propagate RACF requests across the network, each node in the configured network has a pair of `VSAM` files (`INMSG` and `OUTMSG`) to save queued work until it is sent, and its receipt is confirmed by the remote node. These files must be protected.

Rationale:

Disclosure of this information can compromise user credentials and give clues to the protection mechanisms in effect.

Audit:

Display information for all `RRSF` nodes. From the console, specify the `TARGET LIST` command using the prefix you have established for the RACF subsystem. For example, if your prefix is "@". Issue command:

```
@TARGET LIST NODE(*)
```

The file names will be displayed under the `FILE USAGE` heading. For example:

```
FILE USAGE
  "RSFJ.WORK.SYS1.SYS4.INMSG"
    - CONTAINS 0 RECORD(S)
    - OCCUPIES 1 EXTENT(S)
  "RSFJ.WORK.SYS1.SYS4.OUTMSG"
    - CONTAINS 0 RECORD(S)
    - OCCUPIES 1 EXTENT(S)
```

Verify that these data sets are protected with a RACF `DATASET` profile using the `LISTDSD` command. Generally, only the identity of the RACF subsystem requires access. If the subsystem is running with the `TRUSTED` attribute, explicit access is not required. In rare occasions, a system programmer may require `READ` access in order to run the `IRRBRW00` utility.

```
LISTDSD DA('RSFJ.WORK.SYS1.SYS4.INMSG') AUTHUSER GENERIC
```

Also verify that the files are encrypted. Display the encryption status by issuing the command:

```
LISTCAT
```

For example:

```
LISTCAT ENTRY('RSFJ.WORK.SYS1.SYS4.INMSG') ALL
... ENCRYPTIONDATA
  DATA SET ENCRYPTION----- (NO)
...
```

Remediation:

Update the `DATASET` profile as necessary to restrict `UPDATE` access to the RACF subsystem identity (if not running `TRUSTED`) and `READ` access to system programmers who require it.

Encrypting the files requires the standard data set encryption setup (see Additional Information below). Because the RACF subsystem always holds serialization on these files, there is an additional step to perform after the data set encryption setup is complete. The `NEWWORKSPACE` keyword of the `TARGET` command can be used to change the files being used to new ones that are set up for encryption. The same command can be used to restore use of the original files after their encryption setup has been performed.




Default Value:

Data sets are not encrypted.

Additional Information:

1. [Data set encryption](#)
2. [Modifying the attributes of workspace data sets](#)
3. [Health Check RACF_RRSF_RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.10 Ensure the RACF parameter library file is protected (Automated)

Profile Applicability:

- Level 1

Description:

The started procedure in `SYS1.PROCLIB` that starts the RACF subsystem address space contains an optional `RACFPARM DD` statement that identifies a file containing commands to run during subsystem initialization. This file must be protected with a `DATASET` profile.

Rationale:

When these commands execute, they do so under the identity associated with the RACF subsystem, and `OPERCMD`s checking is not performed. Anyone with `UPDATE` access can insert commands.

Audit:

Locate your RACF procedure in the `SYS1.PROCLIB` library. Use the `LISTDS` command to verify that the covering RACF `DATASET` profile has the following attributes:

- `UACC(NONE)`
- No `ID(*)` on the access list
- Not in `WARNING` mode
- `UPDATE` access is restricted to system programmers and/or security personnel
- All `UPDATE` and higher accesses are being logged




Remediation:

Define a covering `DATASET` profile or alter an existing one to adhere to the rules specified above.

Additional Information:

1. [The RACF subsystem](#)
2. [The RACF PROC](#)
3. [The RACF parameter library](#)
4. [Security considerations for the RACF parameter library](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.11 Ensure that RACF remote sharing connections use the TCP/IP protocol (Automated)

Profile Applicability:

- Level 1

Description:

Each individual RACF remote sharing (`RRSF`) connection to a remote node can use either the original `APPC` protocol or the newer `TCP/IP` protocol. `TCP/IP` allows for much stronger protection of the communications using `AT-TLS` technology, complimented by technology such as `z/OS Encryption Readiness Technology (zERT)` that can monitor and enforce the sets of cryptographic algorithms used to protect communications.

Rationale:

`APPC` can only use DES-based encryption, which is far weaker than the encryption offered by `TCP/IP`.

Audit:

The `TARGET` command with the `LISTPROTOCOL` keyword provides a summary of the communication mechanism used for all remote connections.

From the console, specify the `TARGET LIST` command using the prefix you have established for the RACF subsystem. For example, if your prefix is "@". Issue command:

```
@TARGET LISTPROTOCOL
IRRM009I (@) LOCAL RRSF NODE NODE1 SYSNAME SYS1 (MAIN) IS IN THE
          OPERATIVE ACTIVE STATE.

IRRM091I (@) LOCAL NODE TCP LISTENER IS ACTIVE.

IRRM009I (@) LOCAL RRSF NODE NODE1 SYSNAME SYS2 IS IN THE DEFINED
          STATE.

IRRM009I (@) REMOTE RRSF NODE NODE2 SYSNAME SYS3 (MAIN) PROTOCOL TCP
          IS IN THE OPERATIVE ACTIVE STATE.

IRRM009I (@) REMOTE RRSF NODE NODE2 SYSNAME SYS4 PROTOCOL TCP IS IN
          THE OPERATIVE ACTIVE STATE.
```

Remediation:

Establish a plan by which to configure `AT-TLS` protection for `RRSF` connections and convert your `APPC` connections to `TCP/IP`. RACF provides a mechanism by which to seamlessly convert protocols while `RRSF` is in use.

Additional Information:

1. [Establishing RACF security for RRSF TCP/IP connections](#)
2. [Changing the protocol for a connection](#)

2.1.12 Ensure that memory and privileged program dumps are protected (Automated)

Profile Applicability:

- Level 1

Description:

Access to memory and privileged program dumps running Trusted Control Block (TCB) key 0-7 may hold passwords, encryption keys, or other sensitive data that must not be made available.

Rationale:

Failure to control access to these facilities could result in unauthorized personnel modifying sensitive z/OS lists. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Ensure that the Memory and privileged program dumps resources are protected as stated below. Follow these guidelines:

- Ensure that `IEAABD.DMPAUTH` resource and/or generic equivalent is defined and `READ` access is limited to authorized users.
- Ensure that `IEAABD.DMPAUTH` resource and/or generic equivalent `UPDATE` or greater access is restricted to only systems personnel and all access is logged.
- Ensure that `IEAABD.DMPAKEY` resources and/or generic equivalent is defined, and all access is restricted to systems personnel and that all access is logged.

Ensure that resource rules for the above resources and/or generic equivalent specify `UACC(NONE)` and `NOWARNING`.

Remediation:

Define or alter the RACF resource rules for the resources to specify UACC (NONE) and NOWARNING.

Example:

```
RDEF FACILITY IEAABD.DMPAUTH UACC (NONE) OWNER(owner group) AUDIT (ALL (READ) )
```

IEAABD.DMPAUTH.READ access is limited to authorized users that have a valid job duties requirement for access. UPDATE access will be restricted to system programming personnel and access will be logged.

Example:

```
RDEF FACILITY IEAABD.DMPAUTH UACC (NONE) OWNER(owner group) AUDIT (ALL (UPDATE) )  
PERMIT IEAABD.DMPAUTH CLASS (FACILITY) ID(authusers) ACCESS (READ)  
PERMIT IEAABD.DMPAUTH CLASS (FACILITY) ID(syspauDt) ACCESS (UPDATE)
```

IEAABD.DMPAKEY. access will be restricted to system programming personnel and access will be logged.

Example:

```
RDEF FACILITY IEAABD.DMPAKEY.** UACC (NONE) OWNER(owner group)  
AUDIT (ALL (READ) )  
PERMIT IEAABD.DMPAKEY.** CLASS (FACILITY) ID(syspauDt) ACCESS (READ)
```

Default Value:

The resources are not protected.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223654 Rule ID: SV-223654r604139_rule STIG ID: RACF-ES-000060 Severity: CAT II

Additional Information:

1. [Protecting program dumps in the FACILITY class](#)
2. [Health Check RACF SENSITIVE RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.13 Ensure that access to system trace datasets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

`SYS1.TRACE` is used to trace and debug system problems. It can contain sensitive information. In fact, this same consideration applies to any sort of trace log, many of which are application specific.

Rationale:

Unauthorized access to trace files can divulge sensitive system information.

Audit:

Confirm that trace files are covered by a RACF `DATASET` profile with the following attributes:

- UACC(NONE)
- No `ID(*)` on the access list
- Not in `WARNING` mode
- Access is restricted to system programmers and started tasks that perform GTF processing
- All accesses are being logged




Remediation:

Define a covering `DATASET` profile or alter an existing one to adhere to the rules specified above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223671 Rule ID: SV-223671r604139_rule STIG ID: RACF-ES-000230 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.14 Ensure that access to system backup datasets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System backup data sets are necessary for recovery of DASD resident data sets.

Update access to System backup files is limited to system programmers and/or batch jobs that perform DASD backups.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Confirm that trace files are covered by a RACF `DATASET` profile with the following attributes:

- UACC(NONE)
- No `ID(*)` on the access list
- Not in `WARNING` mode
- Access is restricted to system programmers
- All accesses are being logged




Remediation:

Define a covering `DATASET` profile or alter an existing one to adhere to the rules specified above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223670 Rule ID: SV-223670r604139_rule STIG ID: RACF-ES-000220 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.15 Ensure that access to SYSTEM DUMP data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System `DUMP` data sets are used to record system data areas and virtual storage associated with system task failures.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Confirm that trace files are covered by a RACF `DATASET` profile with the following attributes:

- `UACC(NONE)`
- No `ID(*)` on the access list
- Not in `WARNING` mode
- `READ` access is restricted to people required to review these dump data sets for debugging proposes.
- `UPDATE` and higher access is restricted to system programmers
- All accesses are being logged




Remediation:

Define a covering `DATASET` profile or alter an existing one to adhere to the rules specified above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223681 Rule ID: SV-223681r604139_rule STIG ID: RACF-ES-000330 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.16 Ensure that access to SMF collection offload datasets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

SMF backup data sets are those data sets to which SMF data has been offloaded to ensure a historical tracking of individual user accountability. This includes the output of the SMF

Unload utility (IRRADU00). Unauthorized access could result in the compromise of system and customer data.

Rationale:

Minimizing access to a need-to-know basis maintains the integrity and availability of the operating system environment and avoids compromise of the confidentiality of customer data.

Audit:

Confirm that trace files are covered by a RACF `DATASET` profile with the following attributes:

- UACC(NONE)
- No `ID(*)` on the access list
- Not in `WARNING` mode
- READ access is restricted to auditors and other people required to review logging data
- UPDATE and higher access is restricted to system programmers and batch IDs that perform SMF processing
- All accesses are being logged




Remediation:

Define a covering `DATASET` profile or alter an existing one to adhere to the rules specified above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223686 Rule ID: SV-223686r604139_rule STIG ID: RACF-ES-000380 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.1.17 ENSURE that Temporary Data Sets are protected (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS CLASSACT(TEMPDSN)` specifies that the class `TEMPDSN` will be active. When the `TEMPDSN` class is active, access to system-generated temporary data sets is prevented if a temporary data set is allowed to persist after the job which created it has ended. These values become effective immediately after the command `SETROPTS CLASSACT(TEMPDSN)` is issued.

Rationale:

You can protect temporary data sets. Normally, these data sets are considered protected from any accesses except by the job or session that created them, and therefore do not need to be protected by RACF®. However, the following situations could leave a temporary data set unprotected:

- A system failure.
- An initiator failure or initiator termination by the `FORCE` command.
- An automatic restart - between the failure and the restart.

In these cases, if the `TEMPDSN` class is active, only users with the `OPERATIONS` attribute or users authorized to specific `DFSMSdss` functions can scratch any residual `DFP` managed temporary data sets remaining on a volume.

Audit:

Issue the TSO command:

```
SETROPTS LIST
```

Look for the `TEMPDSN` class in 'ACTIVE CLASSES =' session.

Remediation:

Issue the TSO command:

```
SETROPTS CLASSACT(TEMPDSN)
```

Default Value:

The `TEMPDSN` class is inactive.



References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223660 Rule ID: SV-223660r604139_rule STIG ID: RACF-ES-000120 Severity: CAT II

Additional Information:

[Health Check: RACF_TEMPDSN_ACTIVE](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2 Resource Protection

2.2.1 Ensure that the ability to update system dynamic lists are protected (Automated)

Profile Applicability:

- Level 1

Description:

Dynamic lists provide a method of making z/OS system changes without interrupting the availability of the operating system.

Rationale:

Failure to control access to these facilities could result in unauthorized personnel modifying sensitive z/OS lists. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Verify that the accesses for CSV-prefixed resources are restricted. Follow these guidelines:

- RACF resources and/or generic equivalent are defined with a default access of NONE.
- RACF resources and/or generic equivalent identified below will be defined with `AUDIT (ALL (READ))` and `UPDATE` access restricted to system programming personnel:

```
CSVAPF.  
CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC  
CSVAPF.MVS.SETPROG.FORMAT.STATIC  
CSVDYLPA.  
CSVDYNEX.  
CSVDYNEX.LIST  
CSVDYNL.  
CSVDYNL.UPDATE.LNKLST  
CSVLLA.
```

- RACF `CSVDYNEX.LIST` resource and/or generic equivalent will be defined with `AUDIT (FAILURE (READ) SUCCESS (UPDATE))` and `UPDATE` access restricted to system programming personnel.
- RACF `CSVDYNEX.LIST` resource and/or generic equivalent will be defined with `READ` access restricted to auditors.

Remediation:

Create RACF profiles with the appropriate universal access (`UACC`) and access list.

Default Value:

These resources are in the FACILITY class which has a default return code of 4.

Additional Information:

The RACF_SENSITIVE_RESOURCES check which is integrated with the IBM Health Checker for z/OS examines these resources.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223668 Rule ID: SV-223668r604139_rule STIG ID: RACF-ES-000200 Severity: CAT I

Additional Information:

[Health Check RACF_SENSITIVE_RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.2 Ensure that the *GENERIC SETROPTS* value is enabled for *ACTIVE* classes (Automated)

Profile Applicability:

- Level 1

Description:

`GENERIC` controls what classes may have generic profiles. Generic profiles are profiles which cover zero or more resources. They substantially simplify security administration.

Note: It is possible to have characters that would be considered "wildcards", such as '*', '%', '\$', and '&' in non-generic profiles. If the class is not in the `GENERIC` list, then profiles created with wildcards are not generic profiles.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Impact:

Not enabling RACF generic profile processing for a class increases the number of profiles in the RACF data set and makes it less likely that the profile covering a data set is in a RACF cache so I/O to the RACF data base can be avoided.

Audit:

Assure that all `ACTIVE` classes are listed under `GENERIC PROFILE CLASSES`, with the following exceptions:

- Any class which is defined with the `GENERIC=DISALLOWED` attribute as documented in the current version of RACF Macros and Interfaces
- Any class (such as the `CDT`, `KERBLINK`, and `REALM` classes) defined as "generics not recommended" in the RACF Command Language Reference.
- Any class defined with the `GROUP` attribute as documented in the current version of RACF Macros and Interfaces
- Any class defined with the `PROFDEF=NO` attribute as documented in the current version of RACF Macros and Interfaces.

Remediation:

Generic profile processing is activated for the required classes by issuing the command:

```
SETR GENERIC(<classname>)
```




Default Value:

SETR NOGENERIC(classname)

Additional Information:

[See “Protection through generic profiles” in the RACF Security Administrator’s Guide](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>3.3 Configure Data Access Control Lists</u> Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.3 Ensure that IEASYMUP resource is protected (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the System level symbolic resources are defined to the `FACILITY` resource class and protected.

Rationale:

Failure to control access to the `IEASYMUP` resource in use could result in unauthorized personnel modifying sensitive z/OS symbolics. This exposure may threaten the integrity and availability of the operating system environment.

Audit:

Verify that the accesses for `IEASYMUP` resources and/or generic equivalent are restricted. Follow these guidelines:

- RACF resources are defined with a default access of `NONE`.
- RACF resource access authorizations restrict `UPDATE` and/or greater access to DASD administrators, Tape Library personnel, and system programming personnel.
- RACF resource logging requirements are specified.
- RACF resource access authorizations are defined with `UACC(NONE)` and `NOWARNING`.

Remediation:




Ensure that the System level symbolic resources are defined to the `FACILITY` resource class and protected. `UPDATE` access to the System level symbolic resources is limited to System Programmers, DASD Administrators, and/or Tape Library personnel. All access is logged. Ensure the guidelines for the resources and/or generic equivalent are followed.

Limit access to the `IEASYMUP` resources to above personnel with `UPDATE` and/or greater access.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223691 Rule ID: SV-223691r604139_rule STIG ID: RACF-ES-000430

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.4 Ensure that PASSWORD protection for data sets is not used (Manual)

Profile Applicability:

- Level 1

Description:

All protection of system resources must come from RACF.

Rationale:

If multiple protection mechanisms are in place, the accessibility of data, specifically under contingency plan execution, is subject to compromise.

Failure to ensure dataset passwords are not used reduces the integrity and availability of the operating system environment and reduces compromises of confidential customer data.

Audit:

Interview question to check if system `PASSWORD` data set and OS passwords are being used.




Remediation:

Ensure that system `PASSWORD` data set and OS passwords are not used anymore and deleted. All protection must be provided by RACF.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223778 Rule ID: SV-223778r604139_rule STIG ID: RACF-OS-000220 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.5 Ensure that access to datasets in the PARMLIB concatenation is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The z/OS PARMLIB concatenation contains the parameters which control system IPL, configuration characteristics, security facilities, and performance.

Rationale:

Unauthorized UPDATE authority could result in the compromise of the operating system environment, RACF, and customer data. Unauthorized READ authority provides a means for the surveillance and mapping of the system configuration.

Audit:

- Make sure RACF data set rules for the data sets in the PARMLIB concatenation allow appropriate (e.g., global READ) access.
- RACF data set rules for the data set in the PARMLIB concatenation restrict READ, UPDATE and ALTER access to only systems programming and required personnel.
- RACF data set rules for the data sets in the PARMLIB concatenation restrict READ access to only system Level Started Tasks, authorized Data Center personnel, and auditors.
- RACF data set rules for the data sets in the PARMLIB concatenation specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.

Remediation:

Implement controls to specify the valid users authorized to update the SYS1.PARMLIB concatenation. All update and alter access to libraries in the concatenation will be logged using RACF's facilities.

- That systems programming and other required personnel will be authorized to update and alter the PARMLIB concatenation.
- That System Level Started Tasks, authorized Data Center personnel, and auditor can be authorized read access by {The Client}.
- That all update and alter access is logged.

Default Value:

Allow access to datasets.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223697 Rule ID: SV-223697r604139_rule STIG ID: RACF-ES-000500 Severity: CAT I

Additional Information:

The [RACF SENSITIVE RESOURCES](#) health check examines the current `PARMLIB` concatenation for access greater than `READ`.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.6 Ensure that access to all LPA libraries is controlled (Manual)

Profile Applicability:

- Level 1

Description:

LPA modules, once loaded into the Link Pack Area, are capable of performing APF-authorized functions.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

- RACF data set rules for LPA libraries allow appropriate access.
- RACF data set rules for LPA libraries restrict `UPDATE` and/or `ALTER` access to only required personnel.
- RACF data set rules for LPA libraries specify that all (i.e., failures and successes) `UPDATE` and/or `ALTER` access will be logged.

Remediation:




Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes required to protect LPA libraries.

{The Client} will ensure that update and allocate access to LPA libraries is controlled and all update and allocate access is logged.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223678 Rule ID: SV-223678r604139_rule STIG ID: RACF-ES-000300 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.7 Ensure that access to the System Master Catalog is controlled (Manual)

Profile Applicability:

- Level 1

Description:

System master catalogs are the basis for locating all files on the system.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

- RACF data set rules for System Catalogs allow appropriate access.
- RACF data set rules for the Master Catalog restrict greater than READ access to only required personnel.
- RACF data set rules for the Master Catalog specify that all (i.e., failures and successes) greater than `READ` access will be logged.

Remediation:

Ensure that greater than `READ` access to `MASTER CATALOG` is limited to system programmers only and all greater than `READ` access is logged.




Default Value:

Catalog protection defaults are like data set defaults. That is, in the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223666 Rule ID: SV-223666r604139_rule STIG ID: RACF-ES-000180 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.8 Ensure that access to all APF-authorized objects is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The Authorized Program List (APF) designates those libraries that can contain program modules which possess a significant level of security bypass capability.

`extattr +a <program-path-name>` can grant the same capability in the Unix file system.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

RACF data set rules for APF libraries allow appropriate access.

APF libraries should only be accessible in `UPDATE` and/or `ALTER` to z/OS system programmers.

Ensure that the `MVS.SETPROG` and `MVS.SET.PROG` profiles in the `OPERCMDS` class are limited to system programmers. The `BPX.FILEATTR.APF` profile in the `FACILITY` class should also be limited to system programmers.

Failures and successes should be logged for APF libraries.

Remediation:

Ensure that update and allocate access to all APF-authorized libraries are controlled and all update and allocate access is logged.

Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223682 Rule ID: SV-223682r604139_rule STIG ID: RACF-ES-000340 Severity: CAT I

Additional Information:

[Health Check RACF SENSITIVE RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.9 Ensure that access to SYS1.SVCLIB is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The `SYS1.SVCLIB` data set is automatically APF-authorized, contains system SVCs, and may also contain I/O appendages.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Ensure that RACF data set rules for `SYS1.SVCLIB` specify that all (i.e., failures and successes) `UPDATE` and/or `ALTER` access will be logged.

Remediation:

The IAO must ensure that update and allocate access to `SYS1.SVCLIB` is limited to system programmers only and all update and allocate access is logged and reviewed. Periodic reviews of access authorization to critical system files must be performed.
`SYS1.`




Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223675 Rule ID: SV-223675r604139_rule STIG ID: RACF-ES-000270 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.10 Ensure that access to SYS1.IMAGELIB is controlled (Manual)

Profile Applicability:

- Level 1

Description:

`SYS1.IMAGELIB` is a partitioned data set containing universal character set (UCS), forms control buffer (FCB), and printer control information. Most IBM standard UCS images are included in `SYS1.IMAGELIB` during system installation. This data set should be protected as a z/OS system data set.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

- RACF data set rules for `SYS1.IMAGELIB` allow appropriate access.
- RACF data set rules for `SYS1.IMAGELIB` restrict `UPDATE` and/or `ALTER` access to only systems programming personnel.
- RACF data set rules for `SYS1.IMAGELIB` specify that all (i.e., failures and successes) `UPDATE` and/or `ALTER` access will be logged.

Remediation:

{The Client} must ensure that `UPDATE` and/or `ALLOCATE` access to `SYS1.IMAGELIB` is controlled and all update and allocate access is logged.

Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required to protect `SYS1.IMAGELIB`.

`SYS1.IMAGELIB` is automatically APF-authorized. This data set contains modules, images, tables, and character sets which are essential to system print services.




Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223674 Rule ID: SV-223674r604139_rule STIG ID: RACF-ES-000260 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.11 Ensure that access to libraries that contain PPT modules is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Specific PPT (Program Properties Table) designated program modules possess significant security bypass capabilities.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

- RACF data set rules for libraries that contain PPT modules allow appropriate access.
- RACF data set rules for libraries that contain PPT modules restrict `UPDATE` and `ALLOCATE` access to only z/OS systems programming personnel.
- RACF data set rules for libraries that contain PPT modules specify that all `UPDATE` and `ALLOCATE` access will be logged.

Remediation:

Ensure that update and allocate access to libraries containing PPT modules is limited to required personnel only and all update and allocate access is logged.




Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223650 Rule ID: SV-223650r604139_rule STIG ID: RACF-ES-000020 Severity: CAT III

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.12 Ensure that access to SYS1.NUCLEUS is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The `SYS1.NUCLEUS` data set contains a large portion of the system initialization (IPL) programs and pointers to the master and alternate master catalog.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Impact:

Limiting `SYS1.NUCLEUS` authorization to system programmers only allows a program to bypass various levels of security checking.

Audit:

- RACF data set rules for `SYS1.NUCLEUS` allow appropriate access.
- RACF data set rules for `SYS1.NUCLEUS` restrict `UPDATE` and/or `ALTER` access to only z/OS systems programming personnel.
- RACF data set rules for `SYS1.NUCLEUS` specify that all (i.e., failures and successes) `UPDATE` and/or `ALTER` access will be logged.

Remediation:

Ensure that update and allocate access to `SYS1.NUCLEUS` is limited to system programmers only and all update and allocate access is logged.




Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223649 Rule ID: SV-223649r604139_rule STIG ID: RACF-ES-000010 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.13 Ensure that access to all system PROCLIB data sets is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all WRITE and/or greater access to all `PROCLIBs` referenced in the Master JCL and JES2 or JES3 procedure for started tasks (STCs) and TSO logons are restricted to systems programming personnel only.

Rationale:

Unauthorized access to `PROCLIB` data sets referenced in the JES2 procedure can allow unauthorized modifications to STCs and other system level procedures. This could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Refer to the following for the `PROCLIB` data sets that contain the STCs and TSO logons from the following sources:

- `MSTJCLxx` member used during an `IPL`. The `PROCLIB` data sets are obtained from the `IEFPDSI` and `IEFJOBS DD` statements.
- `PROCxx DD` statements and JES2 Dynamic `PROCLIBs`. Where 'xx' is the `PROCLIB` entries for the `STC` and `TSU JOBCLASS` configuration definitions.

Verify that the accesses to the above `PROCLIB` data sets are restricted. Follow these guidelines:

- RACF data set access authorizations restrict `READ` access to all authorized users.
- RACF data set access authorizations restrict `WRITE` and/or greater access to systems programming personnel.

Remediation:

Obtain only the `PROCLIB` data sets that contain `STC` and `TSO` procedures. The data sets to be reviewed are obtained using the following steps:

- All data sets contained in the `MSTJCLxx` member in the DD statement concatenation for `IEFPDSI` and `IEFJOBS`.
- The data set in the `PROCxx` DD statement concatenation that are within the JES2 procedure or identified in the JES2 dynamic `PROCLIB` definitions. The specific `PROCxx` DD statement that is used is obtained from the `PROCLIB` entry for the `JOBCLASSES` of `STC` and `TSU`.




Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223687 Rule ID: SV-223687r604139_rule STIG ID: RACF-ES-000390 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.14 Ensure that System REXX data set is protected (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that read access is restricted to security administrators, systems programmers, and auditors.

Rationale:

Unauthorized access could result in the compromise of passwords, the operating system environment, RACF (Access Control Program), and customer data.

Audit:

Refer to the z/OS system `REXXLIB` concatenation found in `SYS1.PARMLIB (AXR)` for the data set that contains the REXX for Password exit named `IRRPWREX` and the defined `AXRUSER`.

Verify that the data set that contains `IRRPWREX` is restricted. Follow these guidelines:

- RACF data set access authorizations restrict `READ` to `AXRUSER`, z/OS systems programming personnel, security personnel, and auditors.
- RACF data set access authorizations restrict `UPDATE` to security personnel using a documented change management procedure to provide a mechanism for access and revoking of access after use.
- All (i.e., failures and successes) data set access authorities (i.e. `READ`, `UPDATE`, and `CONTROL`) is logged.
- RACF data set access authorizations specify `UACC(NONE)` and `NOWARNING`.

Remediation:

Ensure that there is a procedure documented with the ISSM that defines a change management process to provide mechanism for granting Update access to security administrators on an exception basis. The process should contain procedures to revoke access when documented update is completed.

Ensure all failures and successes data set access authorities for RACF data set that contains the Password exit is logged.

Default Value:

In the absence of a covering data set profile, the `SETROPTS PROTECTALL` value determines the default.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223684 Rule ID: SV-223684r767083_rule STIG ID: RACF-ES-000360 Severity: CAT I

Additional Information:

The [RACF SENSITIVE RESOURCES Health Check](#) examines the protections on System REXX data sets for UPDATE authority.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.15 Ensure that Access to SYS1.LINKLIB is protected (Automated)

Profile Applicability:

- Level 1

Description:

The `SYS1.LINKLIB` data set is automatically APF-authorized, contains system SVCs and the base PPT.

Minimizing access to a need-to-know basis maintains the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

List data set rules for `SYS1.LINKLIB`.

The data set rules for `SYS1.LINKLIB` allows appropriate access.

The data set rules for `SYS1.LINKLIB` restrict `UPDATE` and/or `ALTER` access to only z/OS systems programming personnel.

Remediation:

Ensure that update and allocate access to `SYS1.LINKLIB` is limited to system programmers only and all update and allocate access is logged.

Default Value:

In the absence of a covering profile, the `SETROPTS PROTECTALL` setting determines the access allowed.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223683 Rule ID: SV-223683r604139_rule STIG ID: RACF-ES-000350 Severity: CAT II

Additional Information:

The [RACF SENSITIVE RESOURCES](#) reports on the protections on all of the data sets in the current linklist.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.2.16 Ensure that access to all system-level product installation libraries is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System-level product installation libraries constitute the majority of the systems software libraries.

Limiting `PARMLIB` dataset authorization to system programmers only allows a program to bypass various levels of security checking.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Review the profiles which are covering the libraries for appropriate content.




Remediation:

Ensure that update and allocate access to product libraries is limited to system programmer and other authorized users and all update and allocate access is logged.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223680 Rule ID: SV-223680r604139_rule STIG ID: RACF-ES-000320 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.3 System Settings

2.3.1 Ensure that the *TERMINAL SETROPTS* value is set to *NONE* (Automated)

Profile Applicability:

- Level 1

Description:

`TERMINAL` is used to set the universal access authority (`UACC`) associated with undefined terminals. If you specify `TERMINAL`, but do not specify read or none, the system will prompt you for a value.

Rationale:

The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the command:

```
SETROPTS LIST
```

Look for the following message:

```
ATTRIBUTES = INITSTATS NOWHEN (PROGRAM)  TERMINAL (READ)  SAUDIT CMDVIOL  
NOOPERAUDIT
```

Remediation:

Issue the command:

```
SETROPTS TERMINAL (NONE)
```

Default Value:

`TERMINAL(READ)`




References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 V-262
RACF0330

Additional Information:

[Protecting Undefined Terminals](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.3.2 Ensure that the GENCMD SETROPTS value is enabled for ACTIVE classes (Automated)

Profile Applicability:

- Level 1

Description:

GENCMD controls what classes may have RACF commands update generic profiles.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue TSO command:

```
SETROPTS LIST
```

Look for the following message:

```
INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER xxx DAYS  
or  
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
```

Remediation:

Issue TSO command:

```
PASSWORD (INACTIVE (180) )
```




Default Value:

NOINACTIVE

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 V-260 RACF0310

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.3.3 Ensure that the *PROTECTALL SETROPTS* value is set to *FAIL* (Automated)

Profile Applicability:

- Level 1

Description:

When `PROTECTALL` processing is active and set to `FAIL`, the system automatically rejects any request to create or access a data set that is not RACF-protected. This includes DASD data sets, tape data sets, catalogs, and GDG base names. Temporary data sets that comply with standard MVS temporary data set naming conventions are excluded from `PROTECTALL` processing. `SETROPTS PROTECTALL(FAILURES)` activates `PROTECTALL` processing.

`FAILURES` Specifies that RACF is to reject any request to create or access a data set that is not RACF protected.

`WARNING` Specifies that when a user requests creation of, or access to, a data set that is not RACF protected, RACF allows the request and issues warning messages to the user and the security administrator.

`NOPROTECTALL`

Specifies that a user can create or access a data set that is not protected by a profile. `NOPROTECTALL` is in effect when RACF is using a newly initialized database.

These values become effective immediately as after the command `SETROPTS PROTECTALL(FAILURES)` is issued.

For `PROTECTALL` to work effectively, you must specify `GENERIC` to activate generic profile checking. Otherwise, RACF would allow users to create or access only data sets protected by discrete profiles.

Ensure that no RACF-protected resources will be created or accessed.

Rationale:

If `PROTECTALL` processing is not active, the system grants the ability to create or access a data set that is not RACF-protected. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the ACP control options introduces the possibility of exposure during migration process or contingency plan activation.

Impact:

The performance impact of `PROTECTALL(FAIL)` is negligible.

Audit:

Issue the `SETROPTS LIST` command and look for the following message:

```
PROTECT-ALL IS ACTIVE, CURRENT OPTIONS:
PROTECT-ALL FAIL OPTION IS IN EFFECT
```

Remediation:

Issue the command:

```
SETROPTS PROTECTALL(FAILURES)
```

Default Value:

`NOPROTECTALL`




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223704 Rule ID: SV-223704r604139_rule STIG ID: RACF-ES-000570 Severity: CAT I

Additional Information:

The [RACF_PROTECTALL_FAIL](#) IBM Health Check which is integrated with the IBM Health Checker for z/OS raises an exception if the installation is does not have `PROTECTALL(FAIL)` specified.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4 User Privilege

2.4.1 Ensure that the assignment of the RACF OPERATIONS attribute is tightly controlled (Automated)

Profile Applicability:

- Level 1

Description:

A user possessing the `OPERATIONS` attribute has authorization to do maintenance operations on all RACF-protected data sets, tape volumes, and DASD volumes except those where the access list specifically limits the `OPERATIONS` user to a lower access authority than the operation requires.

Because the `OPERATIONS` and `GROUP-OPERATIONS` privileges allow widespread access they should be limited to users documented with a valid requirement. Delegation of `GROUP-OPERATIONS` processing to other personnel by site-defined Group Administrators is forbidden.

Granting individual authorities using `STGADMIN` profiles in the `FACILITY` class is the preferred method, where applicable. However, there may be cases where `OPERATIONS` is required.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Identify (for example, by using the sample `IRRICE` report named `OPER`, or the Selected User Attribute Report of the data security monitor program) all users with the `OPERATIONS` attribute in their `USER` profile and verify that their need for `OPERATIONS` is justified.

Remediation:

If `OPERATIONS` is not justified, remove it, and grant permissions to only those resources the user requires in order to perform his/her job duties.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223714 Rule ID: SV-223714r604139_rule STIG ID: RACF-ES-000670 Severity: CAT II

Additional Information:

1. [The OPERATIONS attribute](#)
2. [Storage Administration \(STGADMIN\) Profiles in the FACILITY Class or XFACILIT Class](#)
3. [The data security monitor \(DSMON\)](#)
4. [Reports based on the SMF data unload utility \(IRRADU00\)](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>3.3 Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.2 Ensure that TSOAUTH resources are restricted to authorized users (Automated)

Profile Applicability:

- Level 1

Description:

The `TSOAUTH` resource class controls sensitive privileges, such as `OPER`, `ACCOUNT`, `CONSOLE`, `TESTAUTH` and `PARMLIB`. Several of these privileges offer the ability, or provide a facility, to modify sensitive operating system resources.

Rationale:

Failure to control and restrict access to these privileges may result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Confirm that all profiles in the `TSOAUTH` class have the following attributes:

- `UACC(NONE)`
- No `ID(*)` on the access list
- Not in `WARNING` mode

In addition, access to specific resources is restricted to the appropriate job roles as follows:

| | |
|---------------|--|
| Resource name | Authorized personnel |
| ACCT | Security personnel |
| CONSOLE | System programmers, operations staff |
| MOUNT | DASD batch users |
| OPER | System programmers, operations staff |
| PARMLIB | UPDATE to system programmers and READ to auditors |
| TESTAUTH | System programmers who need to debug authorized exits, commands, or programs for your installation |

Remediation:

Alter any covering profile to adhere to the rules specified above.

Default Value:

The `TSOAUTH` class is not active. If a user does not have a TSO segment in their `USER` profile, none of these capabilities apply unless the capabilities are granted by virtue of `SYS1.UADS`.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223836 Rule ID: SV-223836r604139_rule STIG ID: RACF-TS-000010 Severity: CAT II

Additional Information:

1. [Summary of resources protected using RACF](#)
2. [Limiting the use of the TESTAUTH command](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.3 Ensure that access for Surrogate users is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Surrogate users have the ability to submit jobs on behalf of another user (the execution user) without specifying the execution user's password.

Jobs submitted by surrogate users run with the identity of the execution user.

Rationale:

Failure to control surrogate users could result in unauthorized personnel accessing sensitive resources. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

For every `<userID>.SUBMIT` profile in the `SURROGAT` class, verify the following properties:

- UACC(NONE)
- No `ID(*)` on the access list
- Not in `WARNING` mode
- Access is restricted to scheduling tools, started tasks or other system applications required for running production jobs
- Successful accesses are being logged

Remediation:

Alter any `<userID>.SUBMIT` profile as required to confirm to the rules specified above.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223755 Rule ID: SV-223755r604139_rule STIG ID: RACF-JS-000110 Severity: CAT I

Additional Information:

[Allowing surrogate job submission](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.4 Ensure that UID 0 is only assigned to PROTECTED STC IDs (Automated)

Profile Applicability:

- Level 1

Description:

RACF user IDs, groups, and started tasks that use z/OS UNIX facilities are defined to RACF with attributes including UID and GID.

Rationale:

If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Audit:

Search RACF database for all `UID 0` users. Assure that all `UID 0` users are either `STC` IDs or System Administrators.

Issue command:

```
SEARCH CLASS (USER) UID (0)
```

List these users with the `LISTUSER` command and verify that they have the `PROTECTED` attribute.

Remediation:

Assign unique `UIDs` to all users that require Unix access. Use `UNIXPRIV` profiles to provision users with the appropriate Unix access.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223756 Rule ID: SV-223756r604139_rule STIG ID: RACF-JS-000120 Severity: CAT II

Additional Information:

[Using UNIXPRIV class profiles](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.5 Ensure that started tasks requiring exceptional access rights use the TRUSTED attribute and (Automated)

Profile Applicability:

- Level 1

Description:

Some started tasks require access to a broad set of resources, making it impractical to permit the started task to each of these resources individually. In these cases, the security administrator can choose between assigning the `TRUSTED` attribute and the `PRIVILEGED` attribute. While both attributes result in all security checks succeeding, the `TRUSTED` attribute allows for logging those accesses, while `PRIVILEGED` does not. For this reason, `TRUSTED` should be chosen over `PRIVILEGED` except for specialized cases which must be justified.

Rationale:

A lack of logging can result in loss of visibility as to what protected resources a started task is accessing.

Audit:

Display the `STDATA` segment of all profiles in the `STARTED` class, and identify ones running with the `PRIVILEGED` attribute. `RLIST STARTED * STDATA NORACE`

Remediation:

If the use of `PRIVILEGED` cannot be justified, change it to `TRUSTED`:

```
RALTER STARTED <profile-name> STDATA (TRUSTED (YES) PRIVILEGED (NO) )
```

(The change is activated the next time the task is started.)

Default Value:

Both the `TRUSTED` and `PRIVILEGED` attributes are off.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223661 Rule ID: SV-223661r604139_rule STIG ID: RACF-ES-000130 Severity: CAT II

Additional Information:

1. [Using started procedures](#)
2. [Authorizing access to resources](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.6 Ensure that access to Libraries containing EXIT modules is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System exits have a wide range of uses and capabilities within any system. Exits may introduce security exposures within the system, modify audit trails, and alter individual user capabilities.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data, and the potential of a hacker adding a routine to a library and possibly creating an exposure. S.

Audit:

Confirm that data sets containing exit modules are covered by a RACF `DATASET` profile with the following attributes:

- UACC(NONE)
- No `ID(*)` on the access list
- Not in `WARNING` mode
- `UPDATE` and higher access is restricted to system programmers
- `UPDATE` and higher accesses are being logged

Remediation:




Define a covering `DATASET` profile or alter an existing one to adhere to the rules specified above. Issue command:

```
SETROPTS PROTECTALL (FAILURES)
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223679 Rule ID: SV-223679r604139_rule STIG ID: RACF-ES-000310 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.7 Ensure that access to LINKLIST libraries is controlled (Automated)

Profile Applicability:

- Level 1

Description:

The primary function of the LINKLIST is to serve as a single repository for commonly used system modules.

Rationale:

Failure to ensure that the proper set of libraries are designated for LINKLIST can impact system integrity, performance, and functionality. For this reason, controls must be employed to ensure that the correct set of LINKLIST libraries are used. Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Confirm that LINKLIST data sets are covered by a RACF DATASET profile with the following attributes:

- UACC(NONE)
- No ID(*) on the access list
- Not in WARNING mode
- UPDATE and higher access is restricted to system programmers
- UPDATE and higher accesses are being logged

Remediation:

Define a covering DATASET profile or alter an existing one to adhere to the rules specified above.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223683 Rule ID: SV-223683r604139_rule STIG ID: RACF-ES-000350 Severity: CAT II

Additional Information:

[Health Check RACF SENSITIVE RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.8 Ensure that access to SYS1.UADS is maintained (Automated)

Profile Applicability:

- Level 1

Description:

SYS1.UADS is the data set in which emergency user IDs are maintained. This ensures that logon processing can occur even if RACF is not functional.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Audit Procedure: Confirm that SYS1.UADS is covered by a RACF DATASET profile with the following attributes:

- UACC(NONE)
- No ID(*) on the access list
- Not in WARNING mode
- ALTER access is restricted to system programmers
- READ and UPDATE access is restricted to system programmers and/or security administrators

Remediation:

Define a covering DATASET profile or alter an existing one to adhere to the rules specified above.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223667 Rule ID: SV-223667r604139_rule STIG ID: RACF-ES-000190 Severity: CAT I

Additional Information:

[Maintaining the UADS, RACF data base, and broadcast data set](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.9 Ensure that Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Page data sets hold individual pages of virtual storage when they are paged out of real storage.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data. Page datasets access should be limited to system programmers.

Audit:

Retrieve the dataset name of the paging datasets and verify that they are accessible only to the system programmers through the datasets class.




Remediation:

Create dataset profiles protecting the paging datasets.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223688 Rule ID: SV-223688r604139_rule STIG ID: RACF-ES-000400 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.10 Ensure that MCS consoles access is protected through CONSOLE CLASS profile (Manual)

Profile Applicability:

- Level 1

Description:

MCS consoles can be used to issue operator commands. When MCS consoles are configured to force a logon in order to be used, the `CONSOLE` class protect the logon access.

Rationale:

Failure to control access to MCS consoles could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Verify that the `CONSOLE` console-name is accessible only to authorized personnel by issuing command:

```
RLIST CONSOLE console-name ALL
```

Remediation:




Define the console console-name to the `CONSOLE` class and permit the authorized users

```
RDEFINE CONSOLE console-name UACC(NON)  
PERMIT console-name CLASS(CONSOLE) ID(user1 user2...usern) ACCESS(READ)
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223689 Rule ID: SV-223689r816949_rule STIG ID: RACF-ES-000410 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.11 Ensure that access to CONSOLE resources for users in TSOAUTH resource class is restricted (Automated)

Profile Applicability:

- Level 1

Description:

The TSO command `CONSOLE` can be used to establish an extended MCS console session and let the user issue console commands.

Rationale:

Failure to control access to any console could result in unauthorized personnel issuing sensitive operator commands. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Impact:

The `CONSOLE` command in TSO should be restricted to authorized personnel.

Audit:

Verify that the resource `CONSOLE` in the `TSOAUTH` class is only permitted (`READ`) to authorized personnel who will be allowed to establish and extended MCS console session.

```
RLIST TSOAUTH CONSOLE ALL
```

Remediation:

Permit the authorized users only by issuing the command:

```
PERMIT CONSOLE CLASS(TSOAUTH) ID(user1...usern) ACCESS(READ)
```




Or remove the non authorized users by issuing the command:

```
PERMIT CONSOLE CLASS(TSOAUTH) ID(user) DELETE
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223656 Rule ID: SV-223656r604139_rule STIG ID: RACF-ES-000080 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

2.4.12 Ensure that access to system user catalogs is controlled (Automated)

Profile Applicability:

- Level 1

Description:

System catalogs are the basis for locating all files on the system. Software products should be located through specific user catalogs and the user catalogs access should be protected.

Rationale:

Unauthorized access could result in the compromise of the operating system environment, RACF, and customer data.

Audit:

Verify the user catalogs used for software products are only accessible in `READ` mode by the end-users.

The `ICHDSM00` utility can be used to examine protection of the master and user catalogs.

Remediation:




The users not part of the system group should be prevented to access the catalog in more than `READ`, issue command:

```
PERMIT 'user-catalog-profile' ID(user) access(READ)
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223669 Rule ID: SV-223669r811009_rule STIG ID: RACF-ES-000210 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

3 Logging and Auditing

This section describes • How to configure logging to record events • How to aggregate the log of recorded events • How to review the recorded events (auditing) to ensure that the installation security policy is implemented correctly.

3.1 Ensure that the command violations are being logged (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS CMDVIOL` specifies whether RACF is to log violations detected by RACF commands. You must have the `AUDITOR` attribute to specify these options.

`CMDVIOL`

Specifies that RACF is to log violations detected by RACF commands (except `LISTDSD`, `LISTGRP`, `LISTUSER`, `RLIST`, and `SEARCH`) during RACF command processing. A violation might occur because a user is not authorized to modify a particular profile or is not authorized to enter a particular operand on a command.

These values become effective immediately as:

When RACF is using a newly initialized database OR when the command `SETROPTS CMDVIOL` is issued.

Ensure that no RACF-protected resources will be created or accessed.

Rationale:

The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the `SETROPTS LIST` command and look for `CMDVIOL` in `ATTRIBUTES`.

E.g. `ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) SAUDIT CMDVIOL OPERAUDIT`
Issue command:

```
SETROPTS LIST
```

Verify that `CMDVIOL` is listed as one of the `ATTRIBUTES`.

Remediation:

To activate RACF command violation logging issue the command:

```
SETROPTS CMDVIOL
```

Default Value:

`CMDVIOL`




References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 V-257
RACF0280

Additional Information:

[Health Check RACF_AUDIT_CONTROLS](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.2 Ensure that activity of SPECIAL users are being logged (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS SAUDIT` specifies whether RACF is to log RACF commands issued by users with the `SPECIAL` or group `SPECIAL` attribute. You must have the `AUDITOR` attribute to specify these operands.

`SAUDIT`

Specifies that RACF is to log RACF commands (except `LISTDSD`, `LISTGRP`, `LISTUSER`, `RLIST`, and `SEARCH`) issued by users who either had the `SPECIAL` attribute or who gained authority to issue the command through the group-`SPECIAL` attribute.

These values become effective immediately when RACF uses a newly initialized database OR the command `SETROPTS SAUDIT` is issued.

`SAUDIT` specifies whether RACF is to log all RACF commands issued by users with the `SPECIAL` or group `SPECIAL` attribute. The system-wide options control the default settings for determining how RACF will function when handling requests for access to the operating system environment, RACF, and customer data. RACF provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for RACF control options introduces the possibility of exposure during migration process or contingency plan activation.

Ensure that RACF is to log commands issued by a user with `SPECIAL` attribute.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the command:

| |
|----------------------------|
| <code>SETROPTS LIST</code> |
|----------------------------|

Look for `SAUDIT` in `ATTRIBUTE = session:`

E.g. `ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) SAUDIT CMDVIOL OPERAUDIT`

Remediation:

Issue the command:

```
SETROPTS SAUDIT
```

Default Value:

```
SAUDIT
```




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223699 Rule ID: SV-223699r604139_rule STIG ID: RACF-ES-000520 Severity: CAT II

Additional Information:

[Health Check RACF AUDIT CONTROLS](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.3 Ensure that the *AUDIT SETROPTS* value is set for all classes (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS AUDIT(xx)` specifies the names of the classes for which you want RACF to perform auditing. For the classes you specify, RACF logs all uses of the `RACROUTE REQUEST=DEFINE SVC` and all changes made to profiles by RACF commands. When the class specified is `USER`, RACF logs all password and password phrase changes made by `RACROUTE REQUEST=VERIFY`. (RACF adds the classes you specify to those already specified for auditing.) The valid class names are `USER`, `GROUP`, `DATASET`, and those defined in the class descriptor table.

If you specify an asterisk (*), logging occurs for all classes. You must have the `AUDITOR` attribute to enter the `AUDIT` operand. All of the following classes must be audited:

```
AUDIT(DATASET)
AUDIT(GROUP)
AUDIT(USER)
AUDIT(OPERCMDS)
AUDIT(TSOAUTH)
AUDIT(SDSF)
AUDIT(FACILITY)
AUDIT(UNIXPRIV)
AUDIT(***x) for all classes which contain an OSR
AUDIT(PROCESS)
```

These values become effective immediately as:

The command `SETROPTS AUDIT(xx)` is issued

Ensure that RACF audits the classes and log their activities.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the command:

```
SETROPTS LIST
```

Look for the previous mentioned classes in the `AUDIT CLASSES = sessions`.

Remediation:

Issue the command:

```
SETROPTS AUDIT (xx)
```

Where xx is the class that needs to be audited.




To activate logging for all RACF Classes issue the command:

```
SETR AUDIT (*)
```

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 V-255
RACF0260

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.4 Ensure that activities of users with the OPERATIONS attribute are logged (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS OPERAUDIT` specifies whether RACF is to log all actions allowed only because a user has the `OPERATIONS` (or `group-OPERATIONS`) attribute. To perform these actions the `AUDITOR` attribute must be set.

`OPERAUDIT`

Specifies that RACF is to log all actions, such as accesses to resources and commands, allowed only because a user has the `OPERATIONS` or `group-OPERATIONS` attribute.

Once the command `SETROPTS OPERAUDIT` is issued these values become effective immediately.

Ensure that commands issued by users with `OPERATIONS` attribute is logged.

Rationale:

Ensures the user has the correct attribute set to keep an audit of the operations the user runs.

Audit:

Issue the command:

```
SETROPTS LIST
```

Look for `OPERAUDIT` in `ATTRIBUTE = sessions`:

E.g. `ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) SAUDIT CMDVIOL OPERAUDIT`

Remediation:

Issue the command:

```
SETROPTS OPERAUDIT
```

Default Value:

`NOOPERAUDIT`




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223694 Rule ID: SV-223694r604139_rule STIG ID: RACF-ES-000470 Severity: CAT II

Additional Information:

[Health Check RACF AUDIT CONTROLS](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.5 Ensure that Logon statistics are recorded (Automated)

Profile Applicability:

- Level 1

Description:

`SETROPTS INITSTATS` specifies that statistics available during RACF user verification are to be recorded. These statistics include the date and time the user was verified by RACF, the number of user verifications that specified a particular group, and the date and time of the user last requested verification with a particular group. If you specify `INACTIVE`, `REVOKE`, or `WARNING`, `INITSTATS` must be in effect. For applications that specify the `APPL` operand on the `RACROUTE REQUEST=VERIFY` macro, you can define a profile in the `APPL` class to specify that the application needs only daily statistics recorded for its users. To do this, specify the `RACF-INITSTATS(DAILY)` string in the `APPLDATA` field.

Ensure strong security controls by recording statistics of RACF user verification.

Rationale:

If no setting is found, the system-wide defaults will be used. The improper setting of any subsystem fields, individually or in combination with another, can compromise the security of the processing environment. In addition, failure to establish standardized settings for the RACF options introduces the possibility of exposure during migration process or contingency plan activation.

Audit:

Issue the command:

```
SETROPTS LIST
```

Look for `INITSTATS` in `ATTRIBUTES = session:`

E.g. `ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC)`

`INITSTATS` is not listed as one of the `ATTRIBUTES` under `SETR LIST`.

Remediation:




Active `INITSTATS` by issuing the command:

```
SETR INITSTATS
```

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 V-266 RACF0370

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.6 Ensure RACF AUDITOR or ROAUDIT privilege is assigned only to users with auditing mission. (Automated)

Profile Applicability:

- Level 1

Description:

A user having the `AUDITOR` attribute has the authority to specify logging options, gives control of logging SMF data and list auditing information.

Rationale:

With the `AUDITOR` attribute, a user could alter SMF logging data so no trace of the activity could be found. This could destroy audit trace information for RACF system. This attribute should be limited to a minimum number of people. This also applies to the use of Group-Auditor in cases where users are connected to sensitive system dataset HLQ or general resource owning groups with Group-Auditor.

Alternatively, the `ROAUDIT` attribute can be assigned to users who are responsible for auditing RACF but who are not responsible for setting up or changing the auditing options/controls.

Audit:

Assure that only audit team personnel have the `AUDITOR` or `ROAUDIT` attribute. Only audit personnel who are responsible for setting up or changing the auditing options/controls should have the `AUDITOR` attribute.

Remediation:

Remove the `AUDIT` or `ROAUDIT` attribute to users who are not responsible for auditing RACF. Replace the `AUDIT` attribute by the `ROAUDIT` attribute for users who are responsible for auditing RACF but who are not responsible for setting up or changing the auditing options/controls.

Additional Information:

[The AUDITOR attribute](#)

3.7 Ensure that effective SMF records collection options are set (Automated)

Profile Applicability:

- Level 1

Description:

SMF data collection provides a standardized method for recording all system activity to a recording media (file or logstream). including the audit trails from RACF.

Some recording options are mandatory to ensure an effective recording of the activity and therefore complete audit trails.

Rationale:

If the control options for the recording is not set correctly, system audit could be compromised.

Audit:

Using the `D SMF, .O z/OS` command, verify that the following parameters are set:

`ACTIVE` – Ensure SMF recording is to be active.

`JWT (nn)` - Where `nn < 15`. Specifies the maximum amount of time (hhmm) that a job or TSO/E user address space is allowed to wait continuously.

`MAXDORM (0500)` - It specifies the amount of real time (hhmm) that SMF allows data to remain in an SMF buffer before it is written to a recording data set or a log stream

`SYS (DETAIL)` - Specifies the level of SMF data collection for TSO and STC

Remediation:

Modify the `SMFPRMxx` parmlib member to include the recommended options.




Default Value:

```
ACTIVE
JWT(10)
MAXDORM (3000)
SYS (NODETAIL)
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223769 Rule ID: SV-223769r604139_rule STIG ID: RACF-OS-000130 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.8 Ensure that an automated process is in place to collect and retain SMF data (Manual)

Profile Applicability:

- Level 1

Description:

SMF data collection provides a standardized method for recording all system activity to a recording media (file or logstream). including the audit trails from RACF.

Rationale:

Failure to collect and manage adequate retention of SMF records can result in the loss of critical system data.

Audit:

Review SMF data collection and retention processes. Ensure that the processes utilized include a process which is automatically started to dump SMF collection files immediately upon their becoming full.

To ensure that all SMF data is collected in a timely manner, and to reduce the risk of data loss.

Remediation:

Ensure that automated mechanisms are in place to collect and retain all SMF data produced on the system. Dump the SMF files (`MANx`) in systems based on the following guidelines:






1. Dump each SMF file as it fills up during the normal course of daily processing.
2. Dump all remaining SMF data at the end of each processing day.

The same procedure applies if you use `LOGSTREAMS`.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223771 Rule ID: SV-223771r604139_rule STIG ID: RACF-OS-000150 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v8 | 8.10 <u>Retain Audit Logs</u> Retain audit logs across enterprise assets for a minimum of 90 days. | |  |  |

3.9 Ensure that Required SMF data record types is collected (Automated)

Profile Applicability:

- Level 1

Description:

SMF data collection provides a standardized method for recording all system activity to a recording media (file or logstream). including the audit trails from RACF.

All SMF records are uniquely identified by a type and an optional subtype value. The type and subtype values reside in the header portion of the SMF record. A record type can reside in the Standard SMF record header or in the Extended SMF record header. Subtype values always reside in the Standard SMF record header.

From a Security perspective, the following record types are mandatory to be collected30
- Common address space work.

| |
|--|
| 80 - Security Product Processing 81 - RACF Initialization 100/102- Db2 Statistics Db2 Performance 119 - TCP/IP Statistics |
|--|

Rationale:

If the required SMF data record types are not being collected, then accountability cannot be monitored, and its use in the execution of a contingency plan could be compromised.

Audit:

Issue the MVS command:

```
D SMF,O
```

The records that are collected can be found in the parameter `SYS (TYPE (xx:xxx))`
Assure that the active SMF Options dataset contains the following types to be collected:
IBM SMF Records to be collect at a minimum are:

```
0 (00) - IPL
6 (06) - External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) - [SMF] Data Lost
14 (0E) - INPUT or RDBACK Data Set Activity
15 (0F) - OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) - Scratch Data Set Status
18 (12) - Rename Non-VSAM Data Set Status
24 (18) - JES2 Spool Offload
25 (19) - JES3 Device Allocation
26 (1A) - JES Job Purge
30 (1E) - Common Address Space Work
32 (20) - TSO/E User Work Accounting
41 (29) - DIV Objects and VLF Statistics
42 (2A) - DFSMS statistics and configuration
43 (2B) - JES Start
45 (2D) - JES Withdrawal/Stop
47 (2F) - JES SIGNON/Start Line (BSC)/LOGON
48 (30) - JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) - JES Integrity
52 (34) - JES2 LOGON/Start Line (SNA)
53 (35) - JES2 LOGOFF/Stop Line (SNA)
54 (36) - JES2 Integrity (SNA)
55 (37) - JES2 Network SIGNON
56 (38) - JES2 Network Integrity
57 (39) - JES2 Network SYSOUT Transmission
58 (3A) - JES2 Network SIGNOFF
60 (3C) - VSAM Volume Data Set Updated
61 (3D) - Integrated Catalog Facility Define Activity
62 (3E) - VSAM Component or Cluster Opened
64 (40) - VSAM Component or Cluster Status
65 (41) - Integrated Catalog Facility Delete Activity
66 (42) - Integrated Catalog Facility Alter Activity
80 (50) - Security product Processing
81 (51) - RACF Initialization
83 (53) - RACF Audit Record For Data Sets
90 (5A) - System Status
92 (5C) except subtypes 10, 11 - File System Activity
101 (65) - Db2 Accounting
102 (66) - Db2 Performance
103 (67) - IBM HTTP Server
110 (6E) - CICS/ESA Statistics
118 (76) - TCP/IP Statistics
119 (77) - TCP/IP Statistics
123 (7B) - IBM z/OS Connect EE
```




Remediation:

Change the SMFPRMxx member of the SYS1.PARMLIB to collect the necessary record types, then dynamically activates it by issuing the command SET SMF=xx where xx is the last two characters of the member name.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223767 Rule ID: SV-223767r767092_rule STIG ID: RACF-OS-000110 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

3.10 Ensure that RACF audit logs is reviewed on a regular basis (Manual)

Profile Applicability:

- Level 1

Description:

Logging, the recording of data about specific events, is the key to auditing the use of RACF at your installation. But you also need to ensure the logs are reviewed at least daily.

Rationale:

It is very important for any organization to have security logs and actively using them to monitor security-related activities.

Security logs must be monitored and analyzed, even real-time if possible (feeding RACF logs to a SIEM) so attacks can be detected quickly, and appropriate response triggered.

Audit:




Ensure that your auditors are reviewing the RACF events logs at least daily and analyze any security related events (including but not limited to: invalid access attempts, new accounts creation, elevation of privileges, change of identity, access to sensitive resources, ...)

Remediation:

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V-3331 ACP00320

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

3.11 Ensure regular audit of AC=1 modules in APF authorized libraries are conducted (Manual)

Profile Applicability:

- Level 1

Description:

The AC=1 modules that reside in APF authorized libraries should be reviewed annually. It is important maintain documentation identifying the integrity and justification of vendor APF authorized libraries. For non-vendor APF authorized libraries, the source and documentation identifying the integrity and justification that describes the AC=1 module process should be maintained.

Rationale:

Undocumented and/or unauthorized AC=1 modules have a possible risk to the confidentiality, integrity, and availability of the system and present a clear risk to the operating system, RACF, and customer data.

Audit:

Verify the AC=1 documentation and compare it to the actual content of the APF authorized libraries.




Remediation:

Any discrepancy must be fixed: documentation updated and/or libraries/modules removed.

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V-86
STIG ID: AAMV0060

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

3.12 Ensure that only supported (vendor) system software is installed and active on the system (Manual)

Profile Applicability:

- Level 1

Description:

When a vendor drops support of System Software, they no longer maintain security vulnerability patches to the software.

Rationale:

Without vulnerability patches, it is impossible to verify that the system does not contain code which could violate the integrity of the operating system environment.

Audit:

Software products currently running on the reviewed system are at a version less than the products listed in the vendor's Support Lifecycle information.




Remediation:

Upgrade the software found at a version less than the current supported version.
Replace any product out of support.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223781 Rule ID: SV-223781r604139_rule STIG ID: RACF-OS-000250 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 2.1 <u>Establish and Maintain a Software Inventory</u> Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently. |  |  |  |

3.13 Ensure all software on your system is supported (Manual)

Profile Applicability:

- Level 1

Description:

Vendors' code may contain vulnerabilities that may be exploited to cause denial of service or to violate the integrity of the system or data on the System. Most vendors do not develop patches to correct these vulnerabilities on unsupported releases of their software.

Rationale:

With unsupported software on the system, it is impossible to verify that the system does not contain code which could violate the integrity of the operating system environment.

Audit:

Ensure that site has a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support.

Remediation:




Implement a formal migration plan for removing or upgrading OS systems software prior to the date the vendor drops security patch support.

Additional Information:

For IBM products, register for access to the IBM Z and LinuxONE Security Portal.

[System integrity](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently. |  |  |  |

3.14 Implement sensitive z/OS datasets monitoring (Manual)

Profile Applicability:

- Level 1

Description:

It is important to monitor changes, additions or removal from APF and LPA libraries, as well as changes to `SYS1.PARMLIB` PDS members. A monitoring tool should be implemented to monitor the modification to the sensitive z/OS datasets modification.

Rationale:

Impact:

Failure to monitor and review these reports on a regular basis and validating any changes could threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Ensure you are monitoring z/OS sensitive datasets modifications.

Remediation:

Implement a z/OS sensitive dataset monitoring tool like the File Inventory Monitor in IBM Security z/Secure Audit.

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V 23837 ACP00340

Additional Information:

[File integrity monitoring](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|------|
| v8 | 3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal. | | | ● |

4 System Resilience

This section describes how to configure your RACF environment to be resilient against hardware and software errors.

4.1 Ensure that RACF database is backed up on a scheduled basis (Manual)

Profile Applicability:

- Level 1

Description:

If backups of the operating environment are not processed, implementation of a contingency plan would not include the data necessary to fully recover from any outage.

RACF database backups reduce system recovery time.

Rationale:

If regularly scheduled backups of this database are not processed, system recovery time could be unacceptably long.

Audit:

Check with the operation personal that the RACF database is, at least, backed up daily.




Remediation:

Implement a daily backup

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223711 Rule ID: SV-223711r604139_rule STIG ID: RACF-ES-000640 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 11.2 <u>Perform Automated Backups</u> Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. |  |  |  |

4.2 Ensure that RACF primary and backup databases are isolated (Manual)

Profile Applicability:

- Level 1

Description:

RACF backup and recovery data files provide the only means of recovering RACF database in the event of its damage.

Rationale:

In the case where this damage is to the physical volume on which it resides, and any of these recovery data files exist on this volume as well, then complete recovery of the RACF database would be extremely difficult, if even possible.

Audit:

To determine the volume of RACF databases issue the command:

```
RVARY LIST
```

Remediation:

If the alternate database is on the same volume as the primary, it should be re-allocated on another volume.

Copy the active RACF database using `IRRUT200` or `IRRUT400`. The new dataset must be created on a separate volume than the current active database.

Depending upon your configuration, modify the `ICHRDSNT` load module table or the `IRRPRMxx parmlib` member and plan an IPL of the system (or the entire sysplex if in DATASHARING mode).




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223710 Rule ID: SV-223710r604139_rule STIG ID: RACF-ES-000630 Severity: CAT II

Additional Information:

1. [Copy a RACF Database](#)
2. [Configuring a RACF Database](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 11.4 <u>Establish and Maintain an Isolated Instance of Recovery Data</u> Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services. |  |  |  |

4.3 Ensure sensitive data is encrypted (Manual)

Profile Applicability:

- Level 1

Description:

In a z/OS environment, the most effective and compliant way to ensure sensitive data is protected is to implement encryption.

Rationale:

Implementing z/OS dataset encryption would ensure that even privileged users, like storage administrators, if they are not permitted to access the encryption keys, can't access sensitive data

Impact:

On modern machines like z14 or z15, we expect a very limited overhead.

Audit:

Issuing a LISTCAT command to a dataset will display the status of the encryption for this dataset (DATASET ENCRYPTION----(YES) or DATASET ENCRYPTION----(NO))

```
LISTCAT your.dataset.with.sensitive.data
```



Remediation:

Implement z/OS dataset encryption.

Additional Information:

<https://www.redbooks.ibm.com/abstracts/sq248410.html?Open>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. | |  |  |

5 Storage Management

This section describes the Storage Management recommendations.

5.1 Ensure that DFSMS is configured (Manual)

Profile Applicability:

- Level 1

Description:

Configuration properties of DFSMS are specified in various members of the system parmlib concatenation (e.g., SYS1.PARMLIB). Statements within these PDS members provide the execution, operational, and configuration characteristics of the system-managed storage environment.

SYS(x).PARMLIB(IGDSMSxx), SMS parameter settings are specified.

Rationale:

Missing or inappropriate configuration values may result in undesirable operations and degraded security. This exposure could potentially compromise the availability and integrity of some system services and customer data.

Audit:

Verify the the IGDSMSxx parmlib member specify, at least:

```
SMS
ACDS(active dataset name)
COMMDS(communication dataset name)
```




Remediation:

Configure IGDSMSxx according to your policy

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223819 Rule ID: SV-223819r604139_rule STIG ID: RACF-SM-000050 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

5.2 Ensure that a very limited number of users can use the Tape Bypass Label Processing (BLP) (Manual)

Profile Applicability:

- Level 1

Description:

BLP is extremely sensitive, as it allows the circumvention of security access checking for the data. When BLP is used in z/OS, the only verification that is done is for the data set name in the JCL. Any data set name can be used. A user could specify a data set name that he has access to, the job would pass the validation check, and the job would be processed, giving access to the data. BLP is typically used for tapes that are external to the tape management system used on the processor. BLP should be granted to only a limited number of people, preferably the tape librarian and a few key people from the operations staff. If an unauthorized user possesses BLP authority, they could potentially read any restricted tape and modify any information once it has been copied.

Rationale:

If an unauthorized user possesses BLP authority, they could potentially read any restricted tape and modify any information once it has been copied.

Audit:

List the users with access to the `ICHBLP` resource in the `FACILITY` class by issuing the command:

```
SETROPTS LIST
```

Remediation:

Remove any unwanted user.

BLP is controlled thru the `FACILITY` class profile `ICHBLP`

Access is removed with the following command:

```
PE ICHBLP CL(FACILITY) id(<userid>) DELETE
```




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223662 Rule ID: SV-223662r604139_rule STIG ID: RACF-ES-000140 Severity: CAT II

Additional Information:

[Health Check RACF SENSITIVE RESOURCES](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

5.3 Ensure that Automatic Data Set Protection (ADSP) SETROPTS value is set to NOADSP (Manual)

Profile Applicability:

- Level 1

Description:

ADSP indicates that RACF automatically creates discrete data set profiles to protect datasets created by users having this attribute. ADSP specifies that data sets created by users who have the ADSP attribute will be RACF protected automatically. NOADSP cancels automatic RACF protection for users who have ADSP.

Rationale:

Audit:

Issue the command:

```
SETROPTS LIST
```

Look for AUTOMATIC DATASET PROTECTION IS IN EFFECT

Note: NOADSP is the required setting. In the SETROPTS LIST output this will display as AUTOMATIC DATASET PROTECTION IS NOT IN EFFECT.

Remediation:




Issue the command:

```
SETROPTS NOADSP
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223721 Rule ID: SV-223721r604139_rule STIG ID: RACF-ES-000740 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

5.4 Ensure that DFSMS control data sets are protected (Manual)

Profile Applicability:

- Level 1

Description:

DFSMS control data sets provide the configuration and operational characteristics of the system-managed storage environment.

Rationale:

Failure to protect these data sets may result in unauthorized access. This exposure could compromise the availability and integrity of some system services and customer data.

Audit:

Review the `SYS1.PARMLIB(IGDSMS00)` data set to identify the fully qualified file names for the following SMS data sets:

- Source Control Data Set (SCDS)
- Active Control Data Set (ACDS)
- Communications Data Set (COMMDS)
- Automatic Class Selection Routine Source Data Sets (ACS)
- ACDS Backup
- COMMDS Backup

RACF data set rules for the `SCDS`, `ACDS`, `COMMDS`, and `ACS` data sets must restrict `UPDATE` and `ALTER` access to only required z/OS personnel.

Remediation:

Review the `SYS1.PARMLIB(IGDSMS00)` data set to identify the fully qualified file names for the following SMS data sets:

- Source Control Data Set (SCDS)
- Active Control Data Set (ACDS)
- Communications Data Set (COMMDS)
- Automatic Class Selection Routine Source Data Sets (ACS)
- ACDS Backup
- COMMDS Backup

RACF data set rules for the `SCDS`, `ACDS`, `COMMDS`, and `ACS` data sets must restrict `UPDATE` and `ALTER` access to only required z/OS personnel.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223816 Rule ID: SV-223816r604139_rule STIG ID: RACF-SM-000020 Severity: CAT II

6 Networking

This section describes the Networking recommendations.

6.1 CSSMTP Recommendations

This section describes the CSSMTP recommendations.

6.1.1 Ensure CSSMTP Started Task name is configured (Manual)

Profile Applicability:

- Level 1

Description:

IBM CSSMTP requires a started task that will be restricted to certain resources, datasets and other system functions. By defining the started task as a user ID to the system, it allows the SAF to control the access and authorized users that require these capabilities.

Rationale:

Failure to properly control these capabilities could compromise the operating system environment and customer data.

Audit:

Check the `RACFCMDS.RPT(LISTUSER)` report produced by RACF Data Collection to ensure that the IBM CSSMTP started task(s) and/or batch job user ID(s) is(are) defined and is(are) assigned the RACF `PROTECTED` attribute.

Remediation:

The IBM CSSMTP system programmer will ensure that a product's Started Task(s) is(are) properly identified and/or defined to the system SAF.

If the product requires a Started Task, verify that it is properly defined to the System SAF with the proper attributes.

A sample is provided here:

```
adduserCSSMTP name('IBM CSSMTP') owner(stc) dfltgrp(stc) nopass
```




Default Value:

n/a

References:

1. z/OS CSSMTP for RACF STIG :: Version 6, Release: 5 Benchmark Date: 27 Oct 2017
2. Vul ID: V-17452 Rule ID: SV-37480r1_rule STIG ID: ZSMTR030 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |  |  |  |

6.1.2 Ensure CSSMTP Started task(s) is defined to the STARTED resource class. (Manual)

Profile Applicability:

- Level 1

Description:

Access to product resources should be restricted to only those individuals responsible for the application connectivity and who have a requirement to access these resources.

Rationale:

Improper control of product resources could potentially compromise the operating system and customer data.

Audit:

Check the `DSMON.RPT(RACSPT)` report produced by RACF Data Collection to verify that the `IBM CSSMTP` started task(s) is (are) defined to the `STARTED` resource class profile and/or `ICHRIN03` table entry.

Remediation:

The IBM CSSMTP system programmer will ensure that a product's started task(s) is (are) properly identified and/or defined to the System ACP.

A unique user ID must be assigned for the IBM CSSMTP started task(s) through a corresponding `STARTED` class entry.




The following sample set of commands is shown here as a guideline:

```
rdef started CSSMTP.** uacc(none) owner(admin) audit(all(read))
stdata(user(CSSMTP) group(stc))
setr racl(started) ref
```

References:

1. z/OS CSSMTP for RACF STIG :: Version 6, Release: 5 Benchmark Date: 27 Oct 2017
2. Vul ID: V-17454 Rule ID: SV-37483r1_rule STIG ID: ZSMTR032 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.1.3 Ensure AT-TLS protection is enabled for CSSMTP (Manual)

Profile Applicability:

- Level 1

Description:

During the TLS handshake process, mutually acceptable suite of cryptographic algorithms is selected by the server and client. The algorithms specified in the selected suite are used to cryptographically protect the data that subsequently flows between the two. To apply TLS protection of adequate strength, either the CSSMTP application must be configured to use AT-TLS protection, or the JES batch jobs that send mail through CSSMTP must use the STARTTLS command.

Rationale:

Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Impact:

The cryptographic operations involved in TLS do come with a CPU cost. Most of the recommended algorithms are optimized through the use of hardware acceleration. Depending on the number and frequency of TLS handshakes, the CPU impact could be noticeable.

Audit:

Refer to the CSSMTP configuration file specified on the `CONFIG DD` statement in the CSSMTP started task JCL.

Check the following items are in effect for the configuration specified in the `FTP Data` configuration file.

```
- Each `TargetServer` statement specifies the `SECURE YES` parameter  
  
- For any `TargetServer` that does not specify `SECURE YES`, then each JES batch job that sends mail through CSSMTP should use the `STARTTLS` command to specifically request TLS protection of its outbound mail to the target Message Transfer Agent (MTA).
```

Use the `pasearch -t` command to check the AT-TLS policy rule(s) that are configured for each of the endpoints to which CSSMTP connects. While the specific requirements of each rule must accommodate the capabilities of the communication partners (the Mail Transfer Agents) to which CSSMTP connects, you should strive for the use of strong protection. If possible, use settings that require the following:

- TLSv1.2 or a later version of the TLS protocol
- Cipher suites that use:
 - Ephemeral Diffie-Hellman key exchange exchange (ECDHE (preferred) or DHE)
 - AES encryption (AES-GCM preferred)
 - SHA256 or stronger hashes

Remediation:

Review the configuration statements in the CSSMTP configuration file and ensure they conform to the specifications below:

`TargetServer` statement is coded with the `SECURE YES` parameter

For any `TargetServer` statement that is not coded with the `SECURE YES` parameter, check each JES batch job that sends mail through CSSMTP to ensure it uses the `STARTTLS` command before sending its outbound mail to the target Message Transfer Agent (MTA).



NOTE: To identify CSSMTP traffic that is not protected by TLS, you can use the z/OS Communications Server z/OS Encryption Readiness Technology (zERT) function. Use local procedures to configured AT-TLS policy rules for each of the endpoints to which CSSMTP connects. While the specific requirements of each rule must accommodate the capabilities of the communication partners (the Mail Transfer Agents) to which CSSMTP connects, you should strive for the use of strong protection. If possible, use settings that require the following:

- TLSv1.2 or a later version of the TLS protocol
- Cipher suites that use:
 - Ephemeral Diffie-Hellman key exchange (ECDHE (preferred) or DHE)
 - AES encryption (AES-GCM preferred)
 - SHA256 or stronger hashes

Default Value:

No TLS protection is applied.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |

6.1.4 Ensure CSSMTP STC data sets are protected. (Manual)

Profile Applicability:

- Level 1

Description:

The IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC uses privileged functions and accesses to sensitive data. The data sets CSSMTP relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly restrict access to their data sets could result in violating the integrity of the base product which could result in compromising the operating system or sensitive data.

Audit:

Verify that access to the IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets are properly restricted. The data sets to be protected are identified in the data set referenced in the DD statements of the CSSMTP started task(s) and/or batch job(s).

Check that the following guidance is true.

- The RACF data set access authorizations restrict `READ` access to auditors.
- The RACF data set access authorizations restrict `WRITE` and/or greater access to systems programming personnel.
- The RACF data set access authorizations restrict `WRITE` and/or greater access to the product STC(s) and/or batch job(s).
- The RACF data set access authorizations specify `UACC(NONE)` and `NOWARNING`.

Remediation:

Ensure that **WRITE** and/or greater access to the IBM Communications Server Simple Mail Transfer Protocol (CSSMTP) STC data sets are limited to system programmers and CSSMTP STC and/or batch jobs only. **READ** access can be given to auditors at the ISSOs discretion.

The installing Systems Programmer will identify and document the product data sets and categorize them according to who will have what type of access and if required which type of access is logged. The installing systems programmer will identify any additional groups requiring access to specific data sets, and once documented the installing systems programmer will work with the ISSO to see that they are properly restricted to the ACP (Access Control Program) active on the system.

Note: The data sets and/or data set prefixes identified below are examples of a possible installation. The actual data sets and/or prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.




The following commands are provided as an example for implementing data set controls:

```
ad 'sys3.cssmtp.**' uacc(none) owner(sys3) -  
audit(failures(read)) -  
data('CSSMTP Output Data')  
pe 'sys3.cssmtp.**' id(syspauat) acc(a)  
pe 'sys3.cssmtp.**' id(tstcaudt) acc(a)  
pe 'sys3.cssmtp.**' id(smptstc) acc(a)  
pe 'sys3.cssmtp.**' id(audtaudt) acc(r)
```

References:

1. z/OS CSSMTP for RACF STIG :: Version 6, Release: 5 Benchmark Date: 27 Oct 2017
2. Vul ID: V-17067 Rule ID: SV-89725r2_rule STIG ID: ZSMTR001 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.2 FTP Recommendations

This section describes the FTP recommendations.

6.2.1 Ensure FTP Server daemon is configured with proper security parameters (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server daemon requires special privileges and access to sensitive resources to provide its system services. As such, the data sets the FTP Server daemon relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly define and control the FTP Server daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Ensure all of the following items are in effect for the FTP daemon:

1. The FTP daemon is started from a JCL procedure library defined to JES2.
NOTE: The JCL member is typically named `FTPD`
2. The FTP daemon user ID is `FTPD`.
3. The `FTPD` user ID is defined as a `PROTECTED` user ID.
4. The `FTPD` user ID has the following z/OS UNIX attributes: `UID(0)`, `HOME` directory `'/'`, shell program `/bin/sh`.
5. A matching entry in the `STARTED` resource class exists enabling the use of the standard user ID and appropriate group.

Ensure the following items are in effect for all MVS consoles:

1. The FTP daemon user ID must be `FTPD` and a matching entry in the `STARTED` resource class exists enabling the use of the standard user ID and an appropriate group.
2. The `FTPD` user ID is defined as a `PROTECTED` user ID.
3. The `FTPD` user ID has the following z/OS UNIX attributes: `UID(0)`, `HOME` directory `'/'`, shell program `/bin/sh`.

Remediation:

Sample commands to accomplish these requirements are shown here:
Add the FTPD user ID:




```
AU FTPD NAME('STC, FTP Daemon') NOPASSWORD NOOIDCARD DFLTGRP(STCTCPX)
OWNER(STCTCPX) OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))
RDEF STARTED FTPD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
STDATA(USER(=MEMBER) GROUP(STCTCPX) TRACE(YES))
```

Additional permissions may be required. See `SYS1.TCPIP.SEZAINST(EZARACF)` or IBM Communications Server: IP Config Guide.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223742 Rule ID: SV-223742r604139_rule STIG ID: RACF-FT-000100 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.2.2 Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords (Manual)

Profile Applicability:

- Level 1

Description:

During initialization, the FTP daemon reads JCL keywords and configuration files to determine values for critical operational parameters. Because system security is impacted by some of these parameter settings, controlling these options through the configuration file only and explicitly specifying the file locations reduces ambiguity, enhances security auditing, and ensures proper operations.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

a) Display the active started tasks executing on the domain using `SDSF`, or equivalent JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member.

NOTE: The JCL member is typically named `FTPD`.

Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TCP/IP started task JCL.

b) Ensure the following items are in effect for the FTP daemon's started task JCL:

1. The `SYSTCPD` and `SYSFTPD DD` statements specify the TCP/IP Data and FTP Data configuration files respectively.
2. The `ANONYMOUS` keyword is not coded on the `PARM` parameter on the `EXEC` statement.
3. The `ANONYMOUS=logonid` combination is not coded on the `PARM` parameter on the `EXEC` statement.
4. The `INACTIVE` keyword is not coded on the `PARM` parameter on the `EXEC` statement.

c) The `AUTOLOG` statement block can be configured to have TCP/IP start the FTP Server. The FTP entry (e.g., `FTPD`) can include the `PARMSTRING` parameter to pass parameters to the FTP procedure when started.

NOTE: Parameters passed on the `PARMSTRING` parameter override parameters specified in the FTP procedure.

If an FTP entry is configured in the `AUTOLOG` statement block in the TCP/IP Profile configuration file, ensure the following items are in effect:

1. The `ANONYMOUS` keyword is not coded on the `PARMSTRING` parameter.
2. The `ANONYMOUS=logonid` combination is not coded on the `PARMSTRING` parameter.
3. The `INACTIVE` keyword is not coded on `PARMSTRING` parameter.

Remediation:

Review the FTP daemon's started task JCL. Ensure that the `ANONYMOUS` and `INACTIVE` startup parameters are not specified, and configuration file names are specified on the appropriate DD statements.

The FTP daemon program can accept parameters in the JCL procedure that is used to start the daemon. The `ANONYMOUS` and `ANONYMOUS=` keywords are designed to allow anonymous FTP connections. The `INACTIVE` keyword is designed to set the timeout value for inactive connections. Control of these options is recommended through the configuration file statements rather than the startup parameters.

The systems programmer will ensure that the startup parameters for the FTP daemon does not include the `ANONYMOUS`, `ANONYMOUS=`, or `INACTIVE` keywords.

During initialization the FTP daemon searches multiple locations for the `TCPIP.DATA` and `FTP.DATA` files according to fixed sequences. In the daemon's started task JCL, Data Definition (DD) statements will be used to specify the locations of the files. The `SYSTCPD` DD statement identifies the `TCPIP.DATA` file and the `SYSFTPD` DD statement identifies the `FTP.DATA` file.






The systems programmer will ensure that the FTP daemon's started task JCL specifies the `SYSTCPD` and `SYSFTPD` DD statements for configuration files.

It is recommended TCP/IP configuration files reside in `TCPPARMS` datasets or HFS files with restricted access.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223744 Rule ID: SV-223744r604139_rule STIG ID: RACF-FT-000120 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v8 | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |

6.2.3 Ensure FTP.DATA configuration statements enforce secure configuration (Manual)

Profile Applicability:

- Level 1

Description:

The statements in the FTP.DATA configuration file specify the parameters and values that control the operation of the FTP Server components including the use of anonymous FTP. Several of the parameters must have specific settings to provide a secure configuration.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Impact:

Clients that were previously able to connect to the FTP server without TLS protection will no longer be able to do so. In addition, limiting the amount of server information will reduce the amount of server identification information that FTP clients may have previously had access to.

Audit:

a) Refer to the Data configuration file specified on the `SYSFTPD DD` statement in the FTP started task JCL.

b) Ensure the following items are in effect for the configuration statements specified in the FTP Data configuration file:

1. The `ANONYMOUS` statement is not coded (does not exist) or, if it does exist, it is commented out.

NOTE: Other statements prefixed with `ANONYMOUS` may be present. These statements indicate the level of anonymous support and applicable restrictions if anonymous support is enabled using the `ANONYMOUS` statement. These other `ANONYMOUS`-prefixed statements may be ignored.

2. The `INACTIVE` statement is coded with a value between 1 and 900 (seconds).

NOTE: 900 indicates a session timeout value of 15 minutes.

0 disables the inactivity timer check. The default is 300 seconds.

3. The `UMASK` statement is coded with a value of 077.
4. The `BANNER` statement is coded.
5. The `ACCESSERRORMSG` statement is either not coded, is commented out, or is coded with a value of `FALSE`
6. The `REPLYSECURITYLEVEL` statement is coded with a value of 1
7. The `PASSIVEDATACONN` statement is coded with a value of `NOREDIRECT`

Remediation:

Review the configuration statements in the `FTP.DATA` file and ensure they conform to the specifications in the `FTP.DATA CONFIGURATION STATEMENTS` below:

```
STATEMENT NOT CODED,  
CODED WITHOUT VALUE,  
OR PARAMETER VALUE  
  
ANONYMOUS [Not Coded]  
  
BANNER [An HFS file, e.g., /etc/ftp.banner]  
  
INACTIVE [A value between 1 and 900]  
  
UMASK 077 [See Note 1]  
  
ACCESSERRORMSGS [not coded or coded with a value of FALSE]  
  
The REPLYSECURITYLEVEL [coded with a value of 1]  
  
PASSIVEDATACONN [coded with a value of NOREDIRECT]
```

NOTE: If the FTP Server requires a UMASK value less restrictive than 077, requirements should be justified and documented.











Default Value:

See Remediation Procedure. When defaults provide acceptable values, statements may be omitted or commented out. Otherwise, the required values are specified above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223739 Rule ID: SV-223739r604139_rule STIG ID: RACF-FT-000070 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |
| v8 | 4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v8 | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |
| v8 | 13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date. | |  |  |

6.2.4 Ensure AT-TLS protection is enabled for the FTP daemon (Manual)

Profile Applicability:

- Level 1

Description:

During the TLS handshake process, mutually acceptable suite of cryptographic algorithms is selected by the server and client. The algorithms specified in the selected suite are used to cryptographically protect the data that subsequently flows between the two. To apply TLS protection of adequate strength, the FTP daemon must be configured to use AT-TLS protection. Though the FTP daemon was initially implemented to use System SSL directly, that level of support no longer meets acceptable protection standards and is therefore not adequate. In z/OS V2R5, the native support for System SSL was removed from the FTP daemon.

Rationale:

Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Impact:

The cryptographic operations involved in TLS do come with a CPU cost. Most of the recommended algorithms are optimized through the use of hardware acceleration. Depending on the number and frequency of TLS handshakes, the CPU impact could be noticeable.

Audit:

Refer to the Data configuration file specified on the `SYSFTPD DD` statement in the FTPD started task JCL. This is the FTP Data configuration file.

Check the following items are in effect for the configuration specified in the FTP Data configuration file.

NOTE: FIPS 140-2 minimum encryption is the accepted level of encryption and will override this requirement if greater.

- The `EXTENSIONS` statement is coded with the `AUTH_TLS` value
- The `SECURE_FTP` statement is coded with the `REQUIRED` value
- The `SECURE_CTRLCONN` statement is coded with the `PRIVATE` value
- The `SECURE_DATACONN` statement is coded with the `PRIVATE` or `SAFE` value
- The `TLSCERTCROSSCHECK` statement is either not coded, is commented out, or is coded with the `TRUE` value
- The `TLSRFCLEVEL` statement is coded with the `RFC4217` value
- The `TLSMECHANISM` statement is coded with the `ATTLS` value or, if the z/OS version is V2R5 or higher, the `TLSMECHANISM` statement may also be omitted or commented out.

Use the `pasearch -t` command to check the AT-TLS policy rule(s) that are configured for each of the FTP server ports. While the specific requirements of each rule must accommodate the capabilities of the communication partners (the FTP clients) that connect to the server, you should strive for the use of strong protection. If possible, use settings that require the following:

- TLSv1.2 or a later version of the TLS protocol
- Cipher suites that use:
 - Ephemeral Diffie-Hellman key exchange exchange (ECDHE (preferred) or DHE)
 - AES encryption (AES-GCM preferred)
 - SHA256 or stronger hashes

Remediation:

Review the configuration statements in the `FTP.DATA` file and ensure they conform to the specifications in the `FTP.DATA CONFIGURATION STATEMENTS` below:

```
EXTENSIONS [coded with a value of AUTH_TLS]

SECURE_FTP statement is coded with the REQUIRED value

SECURE_CTRLCONN statement is coded with the PRIVATE value

SECURE_DATACONN statement is coded with the PRIVATE or SAFE value

TSLCERTCROSSCHECK [ not coded or coded with a value of TRUE]

TLRSRFCLEVEL [coded with a value of RFC4217]

TLSMECHANISM
```

- If the z/OS version is `V2R4` or earlier [coded with a value of `ATTLS`]
- If the z/OS version is `V2R5` or higher [not coded or coded with a value of `ATTLS`].



Use local procedures to configured AT-TLS policy rules for each of the FTP server ports. While the specific requirements of each rule must accommodate the capabilities of the communication partners (the FTP clients) that connect to the server, you should strive for the use of strong protection. If possible, use settings that require the following:

- TLSv1.2 or a later version of the TLS protocol
- Cipher suites that use:
 - Ephemeral Diffie-Hellman key exchange exchange (ECDHE (preferred) or DHE)
 - AES encryption (AES-GCM preferred)
 - SHA256 or stronger hashes

Default Value:

No TLS protection is applied.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |

6.2.5 Ensure User exits for the FTP Server are not used without approval (Manual)

Profile Applicability:

- Level 1

Description:

Several user exit points in the FTP Server component are available to permit customization of its operating behavior. These exits can be used to modify functions such as FTP command usage, client connection controls, post processing tasks, and SMF record modifications. Proper review and documentation of these exit programs will avoid unintentional compromise of FTP and system security, integrity and availability.

Rationale:

Without proper review and adequate documentation of these exit programs, undesirable operations and degraded security may result. This exposure could lead to unauthorized access impacting data integrity or the availability of some system services or contribute to the loss of accountability and hamper security audit activities.

Impact:

If exits were previously in use, and the reviews find them to be insufficient from a security, integrity or availability point of view, the functions provided by those exits may become unavailable until the exit can be brought up to local standards.

Audit:

1. Refer to the Data configuration file specified on the `SYSFTPD DD` statement in the FTP started task JCL.

Refer to the file(s) allocated by the `STEPLIB DD` statement in the FTP started task JCL. Refer to the libraries specified in the system `LINKLIST` and `LPA`. If any FTP Server exits are in use, identify them and validate that they were reviewed for integrity and approved by the site.

2. Ensure the following items are in effect for FTP Server user exits:

The `FTCHKCMD`, `FTCHKIP`, `FTCHKJES`, `FTCHKPWD`, `FTPSMFEX` and `FTPOSTPR` modules are not located in the FTP daemon's `STEPLIB`, `LINKLIST`, or `LPA`.

NOTE: The `ISPF ISRFIND` utility can be used to search the system `LINKLIST` and `LPA` for specific modules.

- If any FTP Server user exits are implemented, the site must have written approval from site ISSM to install and use the exits.
- If any FTP Server user exits are implemented, the site must have the site systems programmer verify the exit was securely written and installed.

Remediation:



Review the configuration statements in the `FTP.DATA` file. Review the FTP daemon `STEPLIB`, system `LINKLIST`, and Link Pack Area libraries. If FTP Server exits are enabled or present and have not been approved by the site IAM and not securely written and implemented by the site systems programmer, they should not be installed. Verify that none of the following exits are installed unless they have met the requirements listed above:

- `FTCHKCMD`
- `FTCHKIP`
- `FTCHKJES`
- `FTCHKPWD`
- `FTPOSTPR`
- `FTPSMFEX`

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223741 Rule ID: SV-223741r604139_rule STIG ID: RACF-FT-000090 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 2.6 Allowlist Authorized Libraries Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently. | |  |  |

6.2.6 Ensure warning banner for the FTP Server is specified (Manual)

Profile Applicability:

- Level 1

Description:

A logon banner can be used to inform users about the environment during the initial logon. Logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users and advise all users that system use constitutes consent to monitoring.

Rationale:

Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Audit:

1. Refer to the Data configuration file specified on the `SYSETPD DD` statement in the FTP started task `JCL`.
2. Check the `BANNER` statement in the FTP Data configuration file specifies a file or data set that contains a logon banner.

Remediation:

Review the file specified by the `FTP.DATA BANNER` parameter. Ensure the text in this file specifies a logon banner in accordance with the company requirements.

Ensure the `BANNER` statement in the FTP Data configuration file specifies a file or z/OS data set that contains the logon banner.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223736 Rule ID: SV-223736r604139_rule STIG ID: RACF-FT-000040 Severity: CAT II
3. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
4. Vul ID: V-223737 Rule ID: SV-223737r604139_rule STIG ID: RACF-FT-000050 Severity: CAT II

6.2.7 Ensure SMF recording options for the FTP Server are configured (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server can provide audit data in the form of SMF records. The SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Audit:

The system programmer will review the configuration statements in the `FTP.DATA` data set and ensure the SMF options conform to the specifications in the `FTP.DATA` Configuration Statements below or that they are commented out.

```
SMF TYPE119
SMFJES TYPE119
SMFSQL TYPE119
SMFAPPE [Not coded or commented out]
SMFDEL [Not coded or commented out]
SMFEXIT [Not coded or commented out]
SMFLOGN [Not coded or commented out]
SMFREN [Not coded or commented out]
SMFRETR [Not coded or commented out]
SMFSTOR [Not coded or commented out]
```

The FTP Server can provide audit data in the form of SMF records. SMF record type 119, the TCP/IP Statistics record, can be written with the following subtypes:

```
70 - Append
70 - Delete and Multiple Delete
72 - Invalid Logon Attempt
70 - Rename
70 - Get (Retrieve) and Multiple Get
70 - Put (Store and Store Unique) and Multiple Put
```

SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. This data may provide valuable information for security audit activities. Type 119 records use a more standard format and provide more information.

Remediation:

Refer to the Data configuration file specified on the `SYSFTPD DD` statement in the FTP started task JCL.

Ensure the following configuration statement settings are in effect in the FTP Data configuration data set.

Ensure the following items are in effect for the configuration statements specified in the FTP Data configuration file:

The SMF statement is coded with a value of TYPE119.
The SMFJES and SMFSQL statements are coded without any additional values.
The SMFAPPE, SMFDEL, SMFEXIT, SMFLOGN, SMFREN, SMFRETR, and SMFSTOR statements are not coded or commented out.

FTP.DATA Configuration Statements

```
SMF TYPE119
SMFJES TYPE119
SMFSQL TYPE119
SMFAPPE [Not coded or commented out]
SMFDEL [Not coded or commented out]
SMFEXIT [Not coded or commented out]
SMFLOGN [Not coded or commented out]
SMFREN [Not coded or commented out]
SMFRETR [Not coded or commented out]
SMFSTOR [Not coded or commented out]
```

Note: SMF, SMFJES, and SMFSQL may be duplicated in configuration, but one of the entries must specify TYPE119.






Default Value:

See Remediation Procedure. When defaults provide acceptable values, statements may be omitted or commented out. Otherwise, the required values are specified above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223733 Rule ID: SV-223733r604139_rule STIG ID: RACF-FT-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v8 | 8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | |  |  |

6.2.8 Ensure permission and user audit bits for FTP Server are configured. (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server daemon uses privileged functions and accesses sensitive data. The files and directories the FTP daemon relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

The permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table.

```
FTP Server HFS Object Security Settings
File Permission Bits User Audit Bits
/usr/sbin/ftpd 1740 fff
/usr/sbin/ftpdns 1755 fff
/etc/ftp.data 0744 faf
/etc/ftp.banner 0744 faf
```

NOTE: Some of the files listed above may not be used in every configuration.

The `/usr/sbin/ftpd` and `/usr/sbin/ftpdns` objects are symbolic links to `/usr/lpp/tcpip/sbin/ftpd` and `/usr/lpp/tcpip/sbin/ftpdns` respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

The `/etc/ftp.data` file may not be the configuration file the server uses. It is necessary to check the `SYSFTPD DD` statement in the FTP started task JCL to determine the actual file.

The `/etc/ftp.banner` file may not be the banner file the server uses. It is necessary to check the `BANNER` statement in the FTP Data configuration file to determine the actual file. Also, the permission bit setting for this file must be set as indicated in the table above. A more restrictive set of permissions is not permitted.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r-
1 -x
0 --- (most restrictive)
```

The possible audit bits settings are as follows:

- "f log" for failed access attempts
- "a log" for failed and successful access
- no auditing

Remediation:

A systems programmer with `UID(0)` and/or `SUPERUSER` access, will review the UNIX permission bits and user audit bits on the directories and files for the FTP Server. Ensure they conform to the specifications below:

```
FTP Server HFS Object Security Settings
File Permission Bits User Audit Bits
/usr/sbin/ftpd 1740 fff
/usr/sbin/ftpdns 1755 fff
/etc/ftp.data 0744 faf
/etc/ftp.banner 0744 faf
```

The `/usr/sbin/ftpd` and `/usr/sbin/ftpdns` objects are symbolic links to `/usr/lpp/tcpip/sbin/ftpd` and `/usr/lpp/tcpip/sbin/ftpdns` respectively. The permission and user audit bits on the targets of the symbolic links must have the required settings.

The `/etc/ftp.data` file may not be the configuration file the server uses. It is necessary to check the `SYSFTPD DD` statement in the FTP started task JCL to determine the actual file.

The `/etc/ftp.banner` file may not be the banner file the server uses. It is necessary to check the `BANNER` statement in the FTP Data configuration file to determine the actual file.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r-
1 -x
0 --- (most restrictive)
```

The possible audit bits settings are as follows:

- "f log" for failed access attempts
- "a log" for failed and successful access
- no auditing

Some of the files listed above (e.g., `/etc/ftp.data`) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all files that do exist should have the specified permission and audit bit settings.

The following commands can be used (from a user account with an effective `UID(0)`) to update the permission bits and audit bits:

```




chmod 1740 /usr/lpp/tcpip/sbin/ftpd
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpd
chmod 1755 /usr/lpp/tcpip/sbin/ftpdns
chaudit rwx=f /usr/lpp/tcpip/sbin/ftpdns
chmod 0744 /etc/ftp.data
chaudit w=sf,rx+f /etc/ftp.data
chmod 0744 /etc/ftp.banner
chaudit w=sf,rx+f /etc/ftp.banner

```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223734 Rule ID: SV-223734r604139_rule STIG ID: RACF-FT-000020 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.2.9 Ensure MVS data sets for the FTP Server are protected. (Manual)

Profile Applicability:

- Level 1

Description:

The FTP Server daemon uses privileged functions and accesses sensitive data. The data sets the FTP daemon relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of customer data and some system services.

Audit:

The following data set controls must be in effect for the FTP Server:

1. `WRITE` and `ALLOCATE` access to the data set containing the FTP Data configuration file is restricted to systems programming personnel.

NOTE: `READ` access to all authenticated users is permitted.

2. `WRITE` and `ALLOCATE` access to the data set containing the FTP Data configuration file is logged.
3. `WRITE` and `ALLOCATE` access to the data set containing the FTP banner file is restricted to systems programming personnel.
4. `READ` access to the data set containing the FTP banner file is permitted to all authenticated users.

NOTE: The MVS data sets mentioned above may not be used in every configuration. The data set containing the FTP Data configuration file is determined by checking the `SYSFTPD DD` statement in the FTP started task JCL. The data set containing the FTP banner file is determined by checking the `BANNER` statement in the FTP Data configuration file.

Remediation:

Review the data set access authorizations defined to the ACP for the `FTP.DATA` and `FTP.BANNER` files. Ensure these data sets are protected as follows:

The data set containing the `FTP.DATA` configuration file allows read access to all authenticated users and all other access is restricted to systems programming personnel.




All write and allocate access to the data set containing the `FTP.DATA` configuration file is logged.

The data set containing the FTP banner file allows read access to all authenticated users and all other access is restricted to systems programming personnel.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223735 Rule ID: SV-223735r604139_rule STIG ID: RACF-FT-000030 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.2.10 Ensure FTP Control cards are stored in a secure PDS file (Manual)

Profile Applicability:

- Level 1

Description:

FTP control cards carry unencrypted information such as user IDs, passwords and remote IP Addresses. This sensitive credential information should be stored separate from the JCL in a secured PDS.

Rationale:

Without a requirement to store this information separate from the JCL and in-stream JCL, it allows a security exposure by allowing read exposure to this information from anyone having access to the JCL libraries.

Audit:

Provide a list(s) of the locations for all FTP Control cards within a given application, ensuring no FTP control cards are within in-stream JCL, JCL libraries or any open access datasets. List shall indicate which application uses the PDS, and access requirements for those PDS's (who and what level of access). Lists/spreadsheet used for documenting the meeting of this requirement shall be maintained by the responsible Application Security Team, available upon request.

Access to FTP scripts and/or data files located on host system(s) that contain FTP user ID and or password will be restricted to those individuals responsible for the application connectivity and who have a legitimate requirement to know the user ID and password on a remote system.

FTP Control Cards should not be within In-stream JCL, within JCL libraries or open access libraries/datasets.

Anyone having access of read or greater to the FTP control cards must be listed within the spreadsheet by user ID.




Remediation:

Create a list or spreadsheet of the locations where FTP control cards are stored, who should have access to those libraries and which applications the FTP control cards are for.

Add Columns for all people permitted access to the secured PDS.

Make sure that the FTP control Cards for each FTP are stored in a secure PDS and that they are not placed in the JCL libraries or in the in-stream JCL for each FTP.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.3 OpenSSH

This section describes the OpenSSH recommendations.

6.3.1 Ensure SSH daemon is configured to only use the SSHv2 protocol (Manual)

Profile Applicability:

- Level 1

Description:

SSHv1 has many well-known vulnerability exploits and SSH daemon should only use the SSHv2 protocol.

Note: Support for SSHv1 was removed from IBM z/OS OpenSSH in z/OS V2R4. This benchmark only applies to z/OS OpenSSH on releases prior to V2R4, or for installations that use a third party SSH implementation on z/OS.

Rationale:

Exploits of the SSH daemon using the SSHv1 protocol could provide immediate root access to the system.

Impact:

Any clients using SSHv1 (if any) will need to upgrade to SSHv2

Audit:

Locate the SSH daemon configuration file which may be found in /etc/ssh/ directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

Check if SSH Daemon is active.

Examine SSH daemon configuration file. The variables 'Protocol 2,1' or 'Protocol 1' should not be defined on a line without a leading comment.

Remediation:

Edit the `sshd_config` file and set the "Protocol" setting to "2". If any communication partners were using SSHv1, you may need to work with them to coordinate their upgrade to the SSHv2 protocol for accessing your z/OS SSH server.



Default Value:

The z/OS OpenSSH daemon disables SSHv1 by default

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223810 Rule ID: SV-223810r604139_rule STIG ID: RACF-SH-000050 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |

6.3.2 (Optional) Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider where required (Manual)

Profile Applicability:

- Level 1

Description:

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

Rationale:

The FIPS-140 standard requires strict adherence to the use of strong cryptographic algorithms and keys and built-in integrity checks by compliant cryptographic modules.

Audit:

Locate the SSH daemon configuration file which may be found in `/etc/ssh/` directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is active, examine SSH daemon configuration file.

```
sshd_config
```

There should be Ciphers lines and the ciphers list must contain ciphers starting with `aes` and without the `openssh.com` suffix.

The MACs line must be configured to "`hmac-sha-256`" or greater.

The host keys must be stored in a SAF keyring.

Examine the z/OS-specific sshd server system-wide configuration

```
zos_sshd_config
```

Check that the following is true:

```
FIPSMODE YES
CiphersSource ICSF
MACsSource ICSF
```

Remediation:

Edit the SSH daemon configuration and remove any ciphers not starting with `aes` and any with the `openssh.com` suffix. If necessary, add a `Ciphers` line using FIPS 140-2 compliant algorithms.

Configure for message authentication to MACs `hmac-sha-256` or greater.

Store the host keys in a SAF keyring.

Edit the z/OS-specific sshd server system-wide configuration file configuration as follows:

```
FIPSMODE YES
CiphersSource ICSF
MACsSource ICSF
```





Default Value:

FIPS-140 mode is disabled.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223807 Rule ID: SV-223807r803639_rule STIG ID: RACF-SH-000020 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |
| v8 | 16.9 <u>Train Developers in Application Security Concepts and Secure Coding</u> Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers. | |  |  |

6.3.3 Ensure SSH daemon is configured with the logon banner (Manual)

Profile Applicability:

- Level 1

Description:

A logon banner can be used to inform users about the environment during the initial logon. Logon banners are used to warn users against unauthorized entry and the possibility of legal action for unauthorized users and advise all users that system use constitutes consent to monitoring.

Rationale:

Failure to display a logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.

Audit:

Locate the SSH daemon configuration file.

May be found in `/etc/ssh/` directory.

Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is active examine SSH daemon configuration file and check that the Banner statement is configured to something other than none.

The contents of the file specified on the banner statement must contain a logon banner.

Remediation:

Configure the banner statement to a file that contains your company's logon banner. Ensure that the contents of the file specified on the banner statement contain a logon banner.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223809 Rule ID: SV-223809r604139_rule STIG ID: RACF-SH-000040 Severity: CAT II

6.3.4 Ensure SMF recording options for the SSH daemon are configured (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS OpenSSH daemon can provide audit data in the form of SMF records. The SMF data produced by the OpenSSH daemon provides transaction information for both successful and unsuccessful SSH commands.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities and use of the SMF data in the execution of a contingency plan could be compromised.

Audit:

Locate the SSH daemon configuration file which may be found in `/etc/ssh/` directory. Alternately:

From UNIX System Services ISPF Shell navigate to ribbon select tools.

Select option 1 - Work with Processes.

If SSH Daemon is active, examine SSH daemon configuration file.

ServerSMF should be coded with `ServerSMF TYPE119_U83`

Remediation:

Configure the `SERVERSMF` statement in the SSH Daemon configuration file to `TYPE119_U83`.






Default Value:

SMF recording is disabled.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223806 Rule ID: SV-223806r604139_rule STIG ID: RACF-SH-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v8 | 8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | |  |  |

6.3.5 Ensure SSH daemon is configured to use SAF keyrings for key storage (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS OpenSSH daemon supports the storage of asymmetric authentication keys in SAF key rings or z/OS Unix file system files. The SSH keys should be stored in SAF key rings to ensure their protection and to provide for organization access control over the keys.

Rationale:

The use of SAF Key Rings for key storage enforces organizational access control policies and assures the protection of cryptographic keys in storage.

Audit:

Locate the SSH daemon configuration file which may be found in `/etc/ssh/` directory, or from UNIX System Services ISPF Shell navigate to ribbon select tools and select option 1 - Work with Processes.

If SSH Daemon is active examine the file and check the following are either not coded or commented out:

```
#HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
#HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
```

Locate the z/OS-specific sshd server system-wide configuration file `zos_sshd_config` which may be found in `/etc/ssh/` directory.

Check that a `HostKeyRingLabel` line is coded and not commented out.

Remediation:

Configure the SSH Daemon configuration file with the following statements
Ensure that the following is either not coded or comment out.

```
#HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
#HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
```



Configure the `zos_sshd_config` with the `HostKeyRingLabel` Statement.
Example:

```
HostKeyRingLabel="SSHDAEM/SSHDring my label"
```

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V-69237

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | <p>16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u></p> <p>Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p> | |  |  |

6.4 Syslogd Recommendations

This section describes the Syslogd recommendations.

6.4.1 Ensure Syslog daemon is started at z/OS initialization (Manual)

Profile Applicability:

- Level 1

Description:

The Syslog daemon, known as SYSLOGD, is a z/OS UNIX daemon that provides a central processing point for log messages issued by other z/OS UNIX processes. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. It is important that SYSLOGD be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. Finally, syslogd should run in non-swappable mode and under a sufficiently high WLM service class to allow it to keep up with heavy logging loads. If syslogd falls behind, it can cause system instability.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Audit:

Check that the Syslog daemon `SYSLOGD` is started automatically during the initialization of the z/OS system.

NOTE: `SYSLOGD` may be started from the shell, a cataloged procedure (STC), or the `BPXBATCH` program. Additionally, other mechanisms (e.g., `CONTROL-O`) may be used to automatically start the Syslog daemon. To thoroughly analyze this PDI you may need to view the OS SYSLOG using `SDSF`, find the last IPL, and look for the initialization of `SYSLOGD`.

Check that the user ID under which `syslogd` executes is permitted to SAF resource `BPX.STOR.SWAP` in the `FACILITY` class.

Check that the `WLM` service class under which `syslogd` is classified is a high enough to ensure `syslogd` will not starve for dispatching priority.

Remediation:

Review the files used to initialize tasks during system IPL (e.g., `/etc/rc`, `SYS1.PARMLIB`, `CONTROL-O` definitions) to ensure the Syslog daemon is automatically started during z/OS system initialization.

It is important that `syslogd` be started during the initialization phase of the z/OS system to ensure that significant messages are not lost. As with other z/OS UNIX daemons, there is more than one way to start `SYSLOGD`. It can be started as a process in the `/etc/rc` file or as a z/OS started task.

Permit the user ID under which `syslogd` executes to the `BPX.STOR.SWAP` profile in the `FACILITY` class.

Add `syslogd` to the same `WLM` service class or one that is close in dispatching priority.

References:

1. z/OS RACF STIG :: Release: 36 Benchmark Date: 27 Apr 2018 Vuln ID: V-3242

6.4.2 Ensure Syslog daemon is secured (Manual)

Profile Applicability:

- Level 1

Description:

Syslog daemon, known as syslogd, is a zOS UNIX daemon that provides a central processing point for log messages issued by other zOS UNIX processes. It is also possible to receive log messages from other network-connected hosts. Some of the IBM Communications Server components that may send messages to syslog are the FTP and zOS UNIX Telnet servers, AT-TLS and the IKED, NSSD and DMD daemons. The messages may be of varying importance levels including general process information, diagnostic information, critical error notification, and audit-class information. Primarily because of the potential to use this information in an audit process, there is a security interest in protecting the syslogd process and its associated data. The Syslog daemon requires special privileges and access to sensitive resources to provide its system services.

Rationale:

Failure to properly define and control the Syslog daemon could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Check that the Syslog daemon is properly defined and protected as stated below:

- The Syslog daemon user ID is `SYSLOGD`.
- The `SYSLOGD` user ID is defined as a `PROTECTED` user ID.
- The `SYSLOGD` user ID has `UID(0)`, `HOME('/')`, and `PROGRAM('/bin/sh')` specified in the `OMVS` segment.
- A matching entry mapping the `SYSLOGD` started proc to the `SYSLOGD` user ID is in the `STARTED` resource class.
- If Syslog daemon is started from `/etc/rc` then ensure that the `_BPX_JOBNAME` and `_BPX_USERID` environment variables are assigned a value of `SYSLOGD`.

Remediation:

The systems programmer responsible for supporting IBM Communications Server will ensure that Syslog daemon runs under its own user account. Specifically, it does not share the account defined for the z/OS UNIX kernel.

- The Syslog daemon user ID is `SYSLOGD`.
- The `SYSLOGD` user ID is defined as a `PROTECTED` user ID.
- The `SYSLOGD` user ID has `UID(0)`, `HOME('/')`, and `PROGRAM('/bin/sh')` specified in the `OMVS` segment.

To set up and use as an MVS Started Proc, the following sample commands are provided:

```
AU SYSLOGD NAME('stc, tcpip') NOPASSWORD NOOIDCARD DFLTGRP(STC) -  
OWNER(STC) DATA('Reference ISLG0020 for proper setup ')  
ALU SYSLOGD DFLTGRP(stctcp)  
ALU SYSLOGD OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))  
CO SYSLOGD GROUP(stctcp) OWNER(stctcp)
```

A matching entry mapping the `SYSLOGD` started proc to the `SYSLOGD` user ID is in the `STARTED` resource class.




```
RDEF STARTED SYSLOGD.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
STDATA(USER(SYSLOGD) GROUP(STC))
```

If `/etc/rc` is used to start the Syslog daemon ensure that the `_BPX_JOBNAME` and `_BPX_USERID` environment variables are assigned a value of `SYSLOGD`.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223814 Rule ID: SV-223814r604139_rule STIG ID: RACF-SL-000030 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.4.3 Ensure permission and user audit bits for Syslog daemon component are configured. (Manual)

Profile Applicability:

- Level 1

Description:

Directories and files of the Syslog daemon provide the configuration and executable properties of this product. These directories and files must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these objects could lead to unauthorized access. This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

The HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table.

| File | Permission Bits | User Audit Bits |
|--------------------------|-----------------|-----------------|
| SYSLOG Daemon HFS Object | 1740 | fff |
| Security Settings | | |
| /usr/sbin/syslogd | | |

[Configuration File]

```
/etc/syslog.conf 0744 faf
```

[Output log file defined in the configuration file]

```
0744 fff
```

NOTE: The `/usr/sbin/syslogd` object is a symbolic link to `/usr/lpp/tcpip/sbin/syslogd`. The permission and user audit bits on the target of the symbolic link must have the required settings.

The `/etc/syslog.conf` file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file. For example, in `/etc/rc`:

```
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf
```

For example, in the `SYSLOGD` started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) / -f /etc/syslogd.conf'

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f //'SYS1.TCPPARMS(SYSLOG)'''
```

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)
```

The possible audit bits settings are as follows:

- "f log" for failed access attempts
- "a log" for failed and successful access
- no auditing

Remediation:

The systems programmer with `UID(0)` and/or `SUPERUSER` access, will review the UNIX permission bits and user audit bits on the HFS directories and files for the Syslog daemon. Ensure they conform to the specifications in the SYSLOG Daemon HFS Object Security Settings table below.

Log files should have security that prevents anyone except the `syslogd` process and authorized maintenance jobs from writing to or deleting them.

A maintenance process to periodically clear the log files is essential. Logging stops if the target file system becomes full.

SYSLOG Daemon HFS Object Security Settings

| File | Permission Bits | User | Audit Bits |
|--------------------------------|-----------------|------|------------|
| <code>/usr/sbin/syslogd</code> | 1740 | fff | |

[Configuration File]

| | | |
|-------------------------------|------|-----|
| <code>/etc/syslog.conf</code> | 0744 | faf |
|-------------------------------|------|-----|

[Output log file defined in the configuration file]

| | |
|------|-----|
| 0744 | fff |
|------|-----|

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rwX | (least restrictive) |
| 6 | rw- | |
| 3 | -wX | |
| 2 | -w- | |
| 5 | r-X | |
| 4 | r-- | |
| 1 | --X | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

- "f log" for failed access attempts
- "a log" for failed and successful access
- no auditing

NOTE: The `/usr/sbin/syslogd` object is a symbolic link to `/usr/lpp/tcpip/sbin/syslogd`. The permission and user audit bits on the target of the symbolic link must have the required settings.

The `/etc/syslog.conf` file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file. For example, in `/etc/rc`:

| |
|---|
| <code>_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf</code> |
|---|

For example, in the `SYSLOGD` started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) / -f /etc/syslogd.conf'

//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT
// PARM='POSIX(ON) ALL31(ON) /-f //'SYS1.TCPPARMS(SYSLOG)'''
```




The following commands can be used (from a user account with an effective `UID(0)`) to update the permission bits and audit bits:

```
chmod 1740 /usr/lpp/tcpip/sbin/syslogd
chaudit rwx=f /usr/lpp/tcpip/sbin/syslogd
chmod 0744 /etc/syslog.conf
chaudit w=sf,rx+f /etc/syslog.conf
chmod 0744 /log_dir/log_file
chaudit rwx=f /log_dir/log_file
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223812 Rule ID: SV-223812r604139_rule STIG ID: RACF-SL-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.4.4 Ensure syslogd archive data sets are protected (Manual)

Profile Applicability:

- Level 1

Description:

Syslogd can be configured to automatically archive log files to sequential or Generation Data Group (GDG) data sets. These archive data sets contain log information from multiple z/OS system components and must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of sensitive log information from different z/OS system components.

Audit:

Check the following data set controls are in effect for the `syslogd` archive data sets:

1. `WRITE` and `ALLOCATE` access to archive data sets is restricted to the user ID under which `syslogd` runs
2. `READ` access is limited to only those user IDs with legitimate need to access the archived log data.

NOTE: For systems running the TSS ACP replace the `WRITE` and `ALLOCATE` with `WRITE`, `UPDATE`, `CREATE`, `CONTROL`, `SCRATCH`, and `ALL`.

Remediation:




Review the data set access authorizations defined to the ACP for `syslogd` archive data sets. Ensure these data sets are protected in accordance with the following rules:

`WRITE` and `ALLOCATE` access to archive data sets is restricted to the user ID under which `syslogd` runs

`READ` access is limited to only those user IDs with legitimate need to access the archived log data.

NOTE: For systems running the TSS ACP replace the `WRITE` and `ALLOCATE` with `WRITE`, `UPDATE`, `CREATE`, `CONTROL`, `SCRATCH`, and `ALL`.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.5 TCP/IP Recommendations

This section describes the TCP/IP recommendations.

6.5.1 Ensure configuration files for the TCP/IP stack are explicitly specified (Manual)

Profile Applicability:

- Level 1

Description:

The TCP/IP stack reads two configuration files to determine values for critical operational parameters. These file names are specified in multiple locations and, depending on the process, are referenced differently. Because system security is impacted by some of the parameter settings, specifying the file names explicitly in each location reduces ambiguity and ensures proper operations.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task.

If TCPIP is inactive, review the procedure libraries defined to JES2 and locate the TCPIP JCL member.

b) Ensure the following items are in effect for the TCPIP started task JCL:

1. The `PROFILE` and `SYSTCPD DD` statements specify the TCP/IP Profile and Data configuration files respectively.
2. The `RESOLVER_CONFIG` variable on the `EXEC` statement is set to the same file name specified on the `SYSTCPD DD` statement.

Remediation:

Review the TCP/IP started task JCL to ensure the configuration file names are specified on the appropriate DD statements and parameter option.

During initialization the TCP/IP stack uses fixed search sequences to locate the `PROFILE.TCPIP` and `TCPIP.DATA` files. However, uncertainty is reduced, and security auditing is enhanced by explicitly specifying the locations of the files. In the TCP/IP started task's JCL, Data Definition (DD) statements can be used to specify the locations of the files. The `PROFILE DD` statement identifies the `PROFILE.TCPIP` file and the `SYSTCPD DD` statement identifies the `TCPIP.DATA` file.

The location of the `TCPIP.DATA` file can also be specified by coding the `RESOLVER_CONFIG` environment variable as a parameter of the `ENVAR` option in the TCP/IP started task's JCL. In fact, the value of this variable is checked before the `SYSTCPD DD` statement by some processes. However, not all processes (e.g., TN3270 Telnet Server) will access the variable to get the file location; therefore, specifying the file location explicitly, both on a DD statement and through the `RESOLVER_CONFIG` environment variable, reduces ambiguity.

The systems programmer will ensure that the TCP/IP started task's JCL specifies the `PROFILE` and `SYSTCPD DD` statements for the `PROFILE.TCPIP` and `TCPIP.DATA` configuration files and TCP/IP started task's JCL includes the `RESOLVER_CONFIG` variable, set to the name of the file specified on the `SYSTCPD DD` statement.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223827 Rule ID: SV-223827r768725_rule STIG ID: RACF-TC-000080 Severity: CAT II

6.5.2 Ensure TCP/IP stack configuration defined in TCPIP.DATA (Manual)

Profile Applicability:

- Level 1

Description:

During the initialization of TCP/IP servers and clients, the `TCPIP.DATA` configuration file provides information that is essential for proper operations of TCP/IP applications. The `TCPIP.DATA` file acts as the anchor configuration data set for the TCP/IP stack and all TCP/IP servers and clients running in z/OS. During the initialization of TCP/IP servers and clients, the `TCPIP.DATA` file provides basic information that is essential for proper operation.

Rationale:

Inappropriate values could result in undesirable operations and degraded security. This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

Refer to the Data configuration file specified on the `SYSTCPD DD` statement in the TCPIP started task JCL.

Verify that the following configuration statements are specified in the `TCP/IP Data configuration file`.

```
TCPIPJOBNAME
HOSTNAME
DOMAINORIGIN
DATASETPREFIX
```

Remediation:

The system programmer will review the configuration statements in the `TCPIP.DATA` file and ensure they conform to the specifications below:

- `TCPIPJOBNAME` - Specifies the job name of the TCP/IP address space. This name is also used as part of the name of some network security resources.
- `HOSTNAME` - Specifies the TCP/IP host portion of the DNS name of the system.
- `DOMAINORIGIN` - Specifies the default domain name used for DNS searches.
- `DATASETPREFIX` - Specifies the high-level qualifier to be used to dynamically allocate other configuration data sets.

The above `TCPIP.DATA` configuration parameters provide crucial information to TCP/IP applications.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-245536 Rule ID: SV-245536r768737_rule STIG ID: RACF-TC-000100 Severity: CAT II

6.5.3 Ensure Hosts identified by the NSINTERADDR statement are protected (Manual)

Profile Applicability:

- Level 1

Description:

If the hosts identified by `NSINTERADDR` statement are not properly protected they can be stolen, damaged, or disturbed. Without adequate physical security, unauthorized users can access the host and the hosts' components. Therefore, they can interfere with the normal operations of the host.

Rationale:

Improper control of hosts and the hosts' components could compromise network operations.

Audit:

Refer to the Data configuration file specified on the `SYSTCPD DD` statement in the TCPIP started task JCL.

Gather the following information for any `NSINTERADDR` statement coded in the TCP/IP Data configuration file:

Identify the physical location of the host running a DNS server (i.e., on-site or off-site at organization, city, state).

Obtain the description of the physical security controls used to limit access to the area where the host is located.

Remediation:

Verify that if the `NSINTERADDR` statements are not specified in the TCP/IP Data configuration file, this is not applicable.

Verify that the `NSINTERADDR` statements specified in the TCP/IP Data configuration file.

- The `NSINTERADDR` statements refer to hosts connected directly to networks within the physical premises of the host site.
- The `NSINTERADDR` statements refer to hosts that are located in areas with physical access limited to authorized personnel.

Ensure that the hosts and the hosts components identified in the `NSINTERADDR` statement are protected.

Ensure that any `NSINTERADDR` statements coded in the TCPIP.DATA file refer to hosts connected directly to networks within the physical premises of the host site and located in areas with physical access limited to authorized personnel.

6.5.4 Ensure PROFILE.TCPIP configuration statements for the TCP/IP stack are defined (Manual)

Profile Applicability:

- Level 1

Description:

The `PROFILE.TCPIP` configuration file provides system operation and configuration parameters for the TCP/IP stack. Inappropriate values could result in undesirable operations and degraded security.

Rationale:

This exposure may result in unauthorized access impacting data integrity or the availability of some system services.

Audit:

1. Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TCPIP started task JCL.
2. Check that the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the `INCLUDE` statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

1. The `SMFPARMS` statement is not coded or commented out.
2. The `DELETE` statement is not coded or commented out for production systems.
3. The `SMFCONFIG` statement is coded with (at least) the `FTPCLIENT` and `TN3270CLIENT` operands. In addition:
 - a. One or more of the `ZERTDETAIL`, `ZERTSUMMARY` and (for z/OS V2R5 and later) `ZERTDETAILBYPOLICY` are coded. Alternatively, one or more of the `ZERTSERVICE`, `ZERTSUMMARY`, and (for z/OS V2R5 and later) `ZERTSERVICEBYPOLICY` operands may be coded on the `NETMONITOR` statement if a network monitoring product is in use.
 - b. The `TCPSTACK` operand is also recommended.
 - c. The `PROFILE` and `DVIPA` operands are also recommended. Alternatively, `PROFILE` and `SMFSERVICE DVIPA` may be coded on the `NETMONITOR` statement if a network monitoring product is in use.
 - d. If the IPsec protocol is used to protect any z/OS traffic, then `IPSECURITY` is also recommended. Alternatively, `SMFSERVICE IPSECURITY` may be coded on the `NETMONITOR` statement if a network monitoring product is in use.
 - e. If SMC-D is in use, `SMCDLINKEVENT` is also recommended
 - f. If SMC-R is in use, `SMCRLINKEVENT` is also recommended
 - g. If CSSMTP is in use, the `NETMONITOR` statement may be coded with the `SMFSERVICE CSMail CSSMTP` operands.
4. The `TCPCONFIG` statement is coded with (at least) the `RESTRICTLOWPORTS` and `TTLs` operands. Additionally, the `FINWAIT2TIME` operand is coded with a value of 60 or less.
5. The `UDPCONFIG` statement is coded with (at least) the `RESTRICTLOWPORTS` operand. In addition, the `NOUDPCHKSUM` and `NOUDPQUEUELIMIT` operands are not coded.
6. The `IPCONFIG` statement is coded with (at least) the `NODATAGRAMFWD` and `IGNOREREDIRECT` operands. In some cases, there will be a legitimate reason for having `DATAGRAMFWD` coded, but those scenarios should be well understood and documented.
7. The `GLOBALCONFIG` statement is coded with (at least) the `ZERT` operand.
8. The `SACONFIG` statement is coded with (at least) a community name other than "public". In addition, the `SETENABLED` operand must not be specified.

Remediation:

Review the configuration statements in the `PROFILE.TCPIP` file and ensure they conform to the specifications below:

Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the `INCLUDE` statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

1. The `SMFPARMS` statement is not coded or commented out.
2. The `DELETE``` statement is not coded or commented out for production systems.
3. The `SMFCONFIG` statement is coded with (at least) the `FTPCLIENT` and `TN3270CLIENT` operands, as well as the following:
 - a. One or more of the `ZERTDETAIL`, `ZERTSUMMARY` and (for z/OS V2R5 and later) `ZERTDETAILBYPOLICY` are coded. Alternatively, one or more of the `ZERTSERVICE`, `ZERTSUMMARY`, and (for z/OS V2R5 and later) `ZERTSERVICEBYPOLICY` operands may be coded on the `NETMONITOR` statement if a network monitoring product is in use.
 - b. The `TCPSTACK` operand is also recommended.
 - c. The `PROFILE` and `DVIPA` operands are also recommended. Alternatively, `PROFILE` and `SMFSERVICE DVIPA` may be coded on the `NETMONITOR` statement if a network monitoring product is in use.
 - d. If the IPsec protocol is used to protect any z/OS traffic, then `IPSECURITY` is also recommended. Alternatively, `SMFSERVICE IPSECURITY` may be coded on the `NETMONITOR` statement if a network monitoring product is in use.
 - e. If `SMC-D` is in use, `SMCDLINKEVENT` is also recommended
 - f. If `SMC-R` is in use, `SMCRLINKEVENT` is also recommended
 - g. If `CSSMT P` is in use, the `NETMONITOR` statement may be coded with the `SMFSERVICE CSMail CSSMTP` operands.
4. The `TCPCONFIG` statement is coded with (at least) the `RESTRICTLOWPORTS` and `TTLs` operands. Additionally, the `FINWAIT2TIME` operand is coded with a value of 60 or less.
5. The `UDPCONFIG` statement is coded with (at least) the `RESTRICTLOWPORTS` operand and the `NOUDPCHKSUM` and `NOUDPQUEUELIMIT` operands are not coded.
6. The `IPCONFIG` statement is coded with (at least) the `NODATAGRAMFWD` and `IGNOREREDIRECT` operands. In some cases, there will be a legitimate reason for having `DATAGRAMFWD` coded, but those scenarios should be well understood and documented.
7. The `GLOBALCONFIG` statement is coded with (at least) the `ZERT` operand.
8. The `SACONFIG` statement is coded with (at least) a community name other than "public" In addition, the `SETENABLED` operand must not be specified.

| |
|---|
| BASE TCP/IP PROFILE.TCPIP CONFIGURATION STATEMENTS FUNCTIONS |
|---|

`INCLUDE`- Specifies the name of an MVS data set that contains additional `PROFILE.TCPIP` statements to be used

- It Alters the configuration specified by previous statements

SMFPARMS- Specifies SMF logging options for some TCP applications; replaced by **SMFCONFIG**

- Controls collection of audit data

DELETE- Specifies some previous statements, including **PORT** and **PORTRANGE**, that are to be deleted

- Alters the configuration specified by previous statements

SMFCONFIG- - Specifies SMF logging options for Telnet, FTP, TCP, API, and stack activity

- Controls collection of audit data

TCPCONFIG- Specifies various settings for the TCP protocol layer of TCP/IP

- Controls port access














Default Value:

Default values for the various operands varies. Refer to the z/OS Communications Server IP Configuration Reference for the specific default values.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223820 Rule ID: SV-223820r811018_rule STIG ID: RACF-TC-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |
| v8 | 4.7 <u>Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. |  |  |  |
| v8 | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v8 | 8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | |  |  |
| v8 | 13.9 <u>Deploy Port-Level Access Control</u> Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication. | | |  |

6.5.5 Ensure permission and user audit bits for z/OS Unix file system objects that are part of the Base TCP/IP component are configured (Manual)

Profile Applicability:

- Level 1

Description:

z/OS Unix directories and files of the Base TCP/IP component provide the configuration, operational, and executable properties of IBM's TCP/IP system product

Rationale:

Failure to properly secure these objects may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Check that the z/OS Unix file system permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table.

| File | Permission Bits | User Audit Bits |
|---------------------|-----------------|-----------------|
| /etc/hosts | 0744 | faf |
| /etc/protocol | 0744 | faf |
| /etc/resolv.conf | 0744 | faf |
| /etc/services | 0740 | faf |
| /usr/lpp/tcpip/sbin | 0755 | faf |
| /usr/lpp/tcpip/bin | 0755 | faf |

NOTE: Some of the files listed above are not used in every configuration.
The following represents a hierarchy for permission bits from least restrictive to most restrictive:

| | | |
|---|-----|---------------------|
| 7 | rxw | (least restrictive) |
| 6 | rw- | |
| 3 | -wx | |
| 2 | -w- | |
| 5 | r-x | |
| 4 | r-- | |
| 1 | --x | |
| 0 | --- | (most restrictive) |

The possible audit bits settings are as follows:

| | |
|---|--------------------------------------|
| f | log for failed access attempts |
| a | log for failed and successful access |
| - | no auditing |

Remediation:

The systems programmer with `UID(0)` and/or `SUPERUSER` access will review the UNIX permission bits and user audit bits on the HFS directories and files for the Base TCP/IP component. Ensure they conform to the specifications in the BASE TCP/IP z/OS Unix File System Object Security Settings below:

BASE TCP/IP z/OS Unix File System Object Security Settings
File Permission Bits User Audit Bits

```
/etc/hosts 0744 faf
/etc/protocol 0744 faf
/etc/resolv.conf 0744 faf
/etc/services 0740 faf
/usr/lpp/tcpip/sbin 0755 faf
/usr/lpp/tcpip/bin 0755 faf
```

Some of the files listed above (e.g., `/etc/resolv.conf`) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all directories and files that do exist will have the specified permission and audit bit settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)
```

The possible audit bits settings are as follows:

```
f log for failed access attempts
a log for failed and successful access
- no auditing
```

The following commands can be used (from a user account with an effective `UID(0)`) to update the permission bits and audit bits:


```




chmod 0744 /etc/hosts
chaudit w=sf,rx+f /etc/hosts
chmod 0744 /etc/protocol
chaudit w=sf,rx+f /etc/protocol
chmod 0744 /etc/resolv.conf
chaudit w=sf,rx+f /etc/resolv.conf
chmod 0740 /etc/services
chaudit w=sf,rx+f /etc/services
chmod 0755 /usr/lpp/tcpip/bin
chaudit w=sf,rx+f /usr/lpp/tcpip/bin
chmod 0755 /usr/lpp/tcpip/sbin
chaudit w=sf,rx+f /usr/lpp/tcpip/sbin

```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223822 Rule ID: SV-223822r604139_rule STIG ID: RACF-TC-000030 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.5.6 *Ensure access to TCP/IP SAF resources (Manual)*

Profile Applicability:

- Level 1

Description:

The Communication Server access authorization is used to protect TCP/IP resources such as stack, network, port, and other `SERVAUTH` resources. These resources provide additional security checks for TCP/IP users.

Rationale:

Failure to properly secure these TCP/IP resources could lead to unauthorized user access resulting in the compromise of some system services and possible compromise of data.

Impact:

Initial deployment of these measures may cause some applications or users that have legitimate reasons to access a given resource, but were initially unrecognized as such, to be denied access. Once your access control lists are fully developed and verified, this impact will no longer be a factor.

Audit:

Ensure that all TCP/IP resources and/or generic equivalent are properly protected according to the requirements specified.

- The EZA, EZB, and IST resources and/or generic equivalent are defined to the `SERVAUTH` resource class with a `UACC(NONE)`.
- No access is given to the EZA, EZB, and IST high level resources of the `SERVAUTH` resource class.
- If the product CSSMTP is on the system, no access is given to `EZB.CSSMTP` of the `SERVAUTH` resource class.
- If the product CSSMTP is on the system, `EZB.CSSMTP.sysname.writernode.JESnode` will be specified and made available to the CSSMTP started task and authenticated users that require access to use CSSMTP for e-mail services.
- Authenticated users that require access will be permitted access to the second level of the resources in the `SERVAUTH` resource class. Examples are the network (`NETACCESS`), port (`PORTACCESS`), stack (`STACKACCESS`), and FTP resources in the `SERVAUTH` resource class.
- The `EZB.STACKACCESS` resource access authorizations restrict access to those z/OS user IDs with valid requirements for using the specified TCP/IP stack. This control is most useful when multiple TCP/IP stacks are defined on the z/OS system.
- The `EZB.FTP.*.*.ACCESS.HFS` resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access OMVS files and Directories.
- The `EZB.FTP.*.*.ACCESS.JES` resource access authorizations restrict access to FTP users with a specific written documentation showing a valid requirement exists to access FTP JES mode.

Remediation:

Ensure the following items are in effect for TCP/IP resources.

(Note: The resource class, resources, and/or resource prefixes identified below are examples of a possible installation. The actual resource class, resources, and/or resource prefixes are determined when the product is actually installed on a system through the product's installation guide and can be site specific.)

Ensure that the EZA, EZB and IST resources and/or generic equivalent are defined to the `SERVAUTH` resource class with a `UACC(NONE)`

No access is given to the EZA, EZB, and IST resources of the `SERVAUTH` resource class.

If the product `CSSMTP` is on the system, no access is given to `EZB.CSSMTP` of the `SERVAUTH` resource class. `EZB.CSSMTP.sysname.writername.JESnode` will be specified and made available to the `CSSMTP` started task and authenticated users that require access to use `CSSMTP` for e-mail services.

Only authenticated users that require access are permitted access to the second level of the resources in the `SERVAUTH` resource class. Examples are the network (`NETACCESS`), port (`PORTACCESS`), stack (`STACKACCESS`), and FTP resources in the `SERVAUTH` resource class.

The `EZB.STACKACCESS.` resource access authorizations restrict access to those z/OS user IDs with valid requirements for using the specified TCP/IP stack. This control is most useful when multiple TCP/IP stacks are defined on the z/OS system.

The `EZB.FTP.*.*.ACCESS.HFS` resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access z/OS Unix files and directories.

The `EZB.FTP.*.*.ACCESS.JES` resource access authorizations restrict access to FTP users with specific written documentation showing a valid requirement exists to access FTP JES mode.

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

```
RDEF SERVAUTH EZB.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.CSSMTP.sysname.writername.JESnode UACC(NONE) OWNER(ADMIN)
AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.FTP.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.NETACCESS.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.PORTACCESS.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
RDEF SERVAUTH EZB.STACKACCESS.** UACC(NONE) OWNER(ADMIN) AUDIT(FAILURE(READ))
PE EZB.CSSMTP.sysname.writername.JESnode CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.FTP.sysname.ftpstc.ACCESS.HFS CL(SERVAUTH) ID(ftpprofile) ACC(READ)
PE EZB.FTP.sysname.ftpstc.ACCESS.JES CL(SERVAUTH) ID(ftpprofile) ACC(READ)
PE EZB.NETACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.PORTACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
PE EZB.STACKACCESS.** CL(SERVAUTH) ID(authusers) ACC(READ)
```

The following notes apply to these controls:

- To be effective in restricting access, the network (`EZB.NETACCESS`) resource control requires configuration of the `NETACCESS` statement in the `PROFILE.TCPIP` file.

- To be effective in restricting access, the port (`EZB.PORTACCESS`) resource control requires configuration of a `PORT` or `PORTRANGE` statement in the `PROFILE.TCPIP` file. These port definitions within `PROFILE.TCPIP` shall be defined to include `SAF` keyword and a valid name.

A list of possible `SERVAUTH` resources defined to the first two nodes is shown here: (Note that additional resources may be developed with each new release of TCPIP.)

```
ZA.DCAS.
EZB.BINDDVIPARANGE.
EZB.CIMPROV.
EZB.CSSMTP.
EZB.FRCAACCESS.
EZB.FTP.
EZB.INITSTACK.
EZB.IOCTL.
EZB.IPSECCMD.
EZB.LBA.
EZB.MODDVIPA.
EZB.NETACCESS.
EZB.NETMGMT.
EZB.NETSTAT.
EZB.NSS.
EZB.NSSCERT.
EZB.OSM.
EZB.PAGENT.
EZB.PORTACCESS.
EZB.RPCBIND.
EZB.SNMPAGENT.
EZB.SOCKOPT.
EZB.STACKACCESS.
EZB.TN3270.
EZB.TRCCTL.
EZB.TRCSEC.
IST.NETMGMT.
```




Default Value:

Varies by resource. Refer to the z/OS Communications Server IP Configuration Guide, Chapter 3 for a description of each of the resources listed above.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223823 Rule ID: SV-223823r811021_rule STIG ID: RACF-TC-000040 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.5.7 Ensure RACF SERVAUTH resource class is active for TCP/IP resources (Manual)

Profile Applicability:

- Level 1

Description:

IBM Provides the `SERVAUTH` Class for use in protecting a variety of TCP/IP features/functions/products both IBM and third-party. Failure to activate this class will result in unprotected resources.

Rationale:

This exposure may threaten the integrity of the operating system environment and compromise the confidentiality of customer data.

Impact:

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified below.

Audit:

From a command input screen enter:

```
SETROPTS LIST
```

Check that if there are TCP/IP resources defined, the `SERVAUTH` resource class is active.

Remediation:

Ensure that the `SERVAUTH` resource class is active.

The RACF command `SETR LIST` will show the status of RACF controls including a list of `ACTIVE` classes.

The `SERVAUTH` class is activated with the command:

```
SETR CLASSACT (SERVAUTH)
```

Generic profiles and commands should also be enabled with the command:

```
SETR GENERIC (SERVAUTH) GENCMD (SERVAUTH) .
```




Default Value:

The `SERVAUTH` class is inactive.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223824 Rule ID: SV-223824r604139_rule STIG ID: RACF-TC-000050 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.5.8 Ensure Started tasks for the base TCP/IP component are defined securely in RACF (Manual)

Profile Applicability:

- Level 1

Description:

The TCP/IP started tasks require special privileges and access to sensitive resources to provide its system services. Failure to properly define and control these TCP/IP started tasks could lead to unauthorized access.

Rationale:

This exposure may result in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

1. Ensure the following items are in effect for the user ID(s) assigned to the TCP/IP address space(s):
 - a. Named TCPIP or, in the case of multiple instances, prefixed with TCPIP
 - b. Defined as a `PROTECTED` user ID
 - c. z/OS UNIX attributes: `UID(0)`, HOME directory `'/'`, shell program `/bin/sh`
 - d. A matching entry in the `STARTED` resource class exists enabling the use of the standard user ID(s) and appropriate group
2. Ensure the following items are in effect for the user ID assigned to the `EZAZSSI` started task:
 - a. Named `EZAZSSI`
 - b. Defined as a `PROTECTED` user ID
 - c. A matching entry in the `STARTED` resource class exists enabling the use of the standard userid and appropriate group.

Remediation:

1. Define a user ID for the TCPIP Address space. A sample command is shown here:

```
ADDUSER TCPIP NAME('STC, TCPIP') NOPASS DFLTGRP(STCTCPX) OWNER(STCTCPX)  
OMVS(UID(0) HOME('/') PROGRAM('/bin/sh'))
```

2. Define a matching entry in the `STARTED` Class. A sample command is shown here:

```
RDEFINE STARTED TCPIP.** UACC(NONE) OWNER(ADMN) AUDIT(ALL(READ))  
STDATA(USER(TCPIP) GROUP(STCTCPX) TRACE(YES))
```




3. Set up the RACF user ID for the `EZAZSSI` Proc. A sample command to accomplish this is shown here:

```
AU EZAZSSI NAME('STC, EZAZSSI') NOPASS OWNER(STCTCPX) DFLTGRP(STCTCPX)
```

4. Define a matching entry in the `STARTED` class for the `EZAZSSI` proc. A sample command to accomplish this is shown here:

```
RDEF STARTED EZAZSSI.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
STDATA(USER(EZAZSSI) GROUP(STCTCPX) TRACE(YES))
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.5.9 Ensure MVS data sets for the Base TCP/IP component are protected (Manual)

Profile Applicability:

- Level 1

Description:

MVS data sets of the Base TCP/IP component provide the configuration, operational, and executable properties of IBM's TCP/IP system product. The data sets TCP/IP relies upon for its configuration, runtime environment and operation must be properly protected from unauthorized modifications or retrieval to ensure system integrity and privacy of sensitive data.

Rationale:

Failure to properly secure these data sets may lead to unauthorized access resulting in the compromise of the integrity and availability of the operating system environment, ACP, and customer data.

Audit:

Check the following data set controls are in effect for the Base TCP/IP component:

1. `WRITE` and `ALLOCATE` access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix `SYS1.TCPIP.AEZA` and target data sets with the prefix `SYS1.TCPIP.SEZA`).
2. `WRITE` and `ALLOCATE` access to the data set(s) containing the Data and Profile configuration files is restricted to systems programming personnel.

NOTE: If any `INCLUDE` statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

3. `WRITE` and `ALLOCATE` access to the data set(s) containing the Data and Profile configuration files is logged.

NOTE: If any `INCLUDE` statements are specified in the Profile configuration file, the named MVS data sets have the same logging requirements.

4. `WRITE` and `ALLOCATE` access to the data set(s) containing the configuration files shared by TCP/IP applications is restricted to systems programming personnel.

NOTE: For systems running the TSS ACP replace the `WRITE` and `ALLOCATE` with `WRITE`, `UPDATE`, `CREATE`, `CONTROL`, `SCRATCH`, and `ALL`.

Remediation:

Review the data set access authorizations defined to the ACP for the Base TCP/IP component. Ensure these data sets are protected in accordance with the following rules:

WRITE and ALLOCATE access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix `SYS1.TCPIP.AEZA` and target data sets with the prefix `SYS1.TCPIP. SEZA`).

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is restricted to systems programming personnel.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

WRITE and ALLOCATE access to the data set(s) containing the Data and Profile configuration files is logged.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same logging requirements.




WRITE and ALLOCATE access to the data set(s) containing the configuration files shared by TCP/IP applications is restricted to systems programming personnel.

NOTE: For systems running the TSS ACP replace the WRITE and ALLOCATE with WRITE, UPDATE, CREATE, CONTROL, SCRATCH, and ALL.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223826 Rule ID: SV-223826r604139_rule STIG ID: RACF-TC-000070 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

6.6 TN3270 Recommendations

This section describes the TN3270E Telnet Server recommendations.

6.6.1 Ensure configuration statements for the TN3270E Telnet Server are configured. (Manual)

Profile Applicability:

- Level 1

Description:

The TN3270E Telnet Server profile (often called the "Telnet profile") configuration file provides system operation and configuration parameters for the TN3270E Telnet Server. Several of these parameters have potential impact to system security.

Rationale:

Failure to code the appropriate values could result in unexpected operations, degraded security, or unauthorized access impacting data integrity or the availability of some system services.

Audit:

1. Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TN3270E Telnet Server started task JCL.
2. Ensure the following items are in effect for the configuration statements specified in the Telnet profile:

NOTE: If the `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

`TELNETGLOBAL` block (only one defined)

- If the `TNSACONFIG` statement is specified, the `COMMUNITY` parameter is specified with a value other than "public"

`TELNETPARMS` block (one defined for each port the server is listening to, typically ports 23 and 992)

- The `TELNETPARMS INACTIVE` and `KEEPINACTIVE` statements are coded within each `TELNETPARMS` statement block and specifies a value between 1 and 900.

NOTE: The `INACTIVE` and `KEEPINACTIVE` statements can appear in any of the `TELNETGLOBALS`, `TELNETPARMS` and `PARMSGROUP` statement blocks.

- The `TELNETPARMS TKOSPECLURECON` statement is not coded or commented out.

NOTE: The `TKOSPECLURECON` statement can appear in any of the `TELNETGLOBALS`, `TELNETPARMS` and `PARMSGROUP` statement blocks.

`BEGINVTAM` block (one or more defined)

- The `BEGINVTAM RESTRICTAPPL` statement is either not coded or is commented out.

Remediation:

Review the configuration statements in the Telnet profile and ensure they conform to the specifications below:

NOTE: If the `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

The `TNSACONFIG` statement, if used, specifies the `COMMUNITY` parameter with a value other than "public"

`TELNETPARMS` block (one defined for each port the server is listening to, typically ports 23 and 992)

The `TELNETPARMS INACTIVE` and `KEEPINACTIVE` statements are coded within each `TELNETPARMS` statement block and specifies a value between 1 and 900.

`INACTIVE` and `KEEPINACTIVE` statements should not be coded with a value greater than 900 or 0. 0 disables the inactivity timer check.

NOTE: The `INACTIVE` and `KEEPINACTIVE` statement can appear in both `TELNETGLOBAL` and `TELNETPARM` statement blocks.

The `TELNETPARMS TKOSPECLURECON` statement should not be coded or it should be commented out.

`BEGINVTAM` block (one or more defined)

The `BEGINVTAM RESTRICTAPPL` statement is not coded or it should be commented out.









Default Value:

The defaults vary per statement. Refer to the z/OS Communications Server IP Configuration Reference for details.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223835 Rule ID: SV-223835r604139_rule STIG ID: RACF-TN-000060 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v8 | <u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. |  |  |  |
| v8 | <u>13.5 Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date. | |  |  |

6.6.2 Ensure VTAM session setup controls for the TN3270E Telnet Server are configured (Manual)

Profile Applicability:

- Level 1

Description:

After a connection from a Telnet client to the TN3270E Telnet Server has been established, the process of session setup with a VTAM application occurs. A number of `BEGINVTAM` statements must be coded in a specific configuration to ensure adequate control to VTAM applications is maintained. The appropriate statements must be coded to ensure adequate security of the established SNA sessions.

Rationale:

Failure to code the appropriate statements could result in unauthorized access to the host and application resources. This exposure may impact data integrity or the availability of some system services.

Audit:

a) Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TN3270E Telnet Server started task JCL. The TN3270E Telnet Server profile is often called the "Telnet profile."

b) Ensure the following items are in effect for the configuration statements specified in the Telnet profile file:

NOTE: If the `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

1. Within each `BEGINVTAM` statement block, one `BEGINVTAM USSTCP` statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.
2. The USS table specified on each "backstop" `USSTCP` statement mentioned in Item (1) above is coded to allow access only to session manager applications and NC PASS applications.
3. Within each `BEGINVTAM` statement block, additional `BEGINVTAM USSTCP` statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.
4. Any `BEGINVTAM DEFAULTAPPL` statement that does not specify a client identifier or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC PASS application as the application name.
5. Any `BEGINVTAM LUMAP` statement, if used with the `DEFAPPL` operand and applied to unsecured terminals, specifies only a session manager application or an NC PASS application.

NOTE: The `BEGINVTAM LINEMODEAPPL` requirements are not reviewed here. Further testing must be performed to determine how the `CL/Supersession` and `NC-PASS` applications work with line mode.

Remediation:

Review the `BEGINVTAM` configuration statements in the Telnet profile. Ensure they conform to the specifications below.

NOTE: If the `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

Within each `BEGINVTAM` statement block, one `BEGINVTAM USSTCP` statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.

The USS table specified on each “backstop” `USSTCP` statement mentioned above is coded to allow access only to session manager applications and NC PASS applications. Within each `BEGINVTAM` statement block, additional `BEGINVTAM USSTCP` statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.

Any `BEGINVTAM DEFAULTAPPL` statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC PASS application as the application name.

For z/OS systems, any `BEGINVTAM LUMAP` statement, if used with the `DEFAPPL` operand and applied to unsecured terminals, specifies only a session manager application or an NC PASS application.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223834 Rule ID: SV-223834r604139_rule STIG ID: RACF-TN-000050 Severity: CAT II

Additional Information:

After a connection from a Telnet client to the TN3270 Telnet Server has been established, the process of session setup with a VTAM application occurs. A number of `BEGINVTAM` statements will be coded in a specific configuration to ensure that adequate control over access to VTAM applications is maintained.

Connections originate from secure terminals or unsecured terminals. The TN3270 Telnet Server should be configured to address these two types of connections. Terminals should meet two conditions to be considered secure. One condition involves the hardware and configuration. Secure terminals include devices that are directly attached to the host, such as 3270-type terminals coax connected to a 3174 Control Unit. They also include PCs running 3270 terminal emulation clients attached to a private LAN (i.e., a LAN without access to an external network such as the `NIPRNet`). The other condition involves the location of the terminals. Secure terminals are located in areas with physical access limited to authorized personnel. Examples of terminals that are not secure are those attached via the `NIPRNet` or via dial-in servers. The intent of this distinction is to allow additional connection options (e.g., bypassing session manager control) to authorized personnel working in controlled access areas. These connection options may be necessary for operational control or for system recovery procedures.

The `BEGINVTAM USSTCP` statement can be used to specify a customized Unformatted System Services (USS) table for client connections. The USS table can provide a level of access control by restricting the commands that allow connections to VTAM applications. The USS table specified by the `USSTCP` statement can be the same as the one used by the SNA component of IBM Communications Server.

The `BEGINVTAM DEFAULTAPPL` statement can be used to specify the VTAM application to which a client is automatically connected when a session is established using a protocol other than linemode protocol.

The `BEGINVTAM LUMAP` statement can specify a default VTAM application using the `DEFAPPL` operand. This processing is similar to the `DEFAULTAPPL` and `LINEMODEAPPL` processing, except that a client identifier should be coded. When a client matches the `LUMAP` specification, the `DEFAPPL` specification overrides the `DEFAULTAPPL` or `LINEMODEAPPL` specifications.

6.6.3 Ensure Warning banner for the TN3270 Telnet Server is configured (Manual)

Profile Applicability:

- Level 1

Description:

A logon banner can be used to inform users about the environment during the initial logon. For example, the logon banners can be used to warn users against unauthorized entry and the possibility of legal action for unauthorized users and advise all users that system use constitutes consent to monitoring.

Rationale:

Failure to display a logon warning banner without this type of information could adversely impact the ability to prosecute unauthorized users and users who abuse the system.

Audit:

- a) Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TN3270E Telnet Server started task JCL.
- b) Ensure that all USS tables referenced in `BEGINVTAM USSTCP` statements include MSG10 text that specifies a logon banner.

Remediation:

Review all USS tables referenced in `BEGINVTAM USSTCP` statements in the Telnet profile. Ensure the MSG10 text specifies a logon banner.

Within the TN3270 Telnet Server, the banner can be implemented through the USS table that is specified on a `BEGINVTAM USSTCP` statement. The text associated with message ID 10 (i.e., MSG10) in the USS table is sent to clients that are subject to `USSTCP` processing.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223833 Rule ID: SV-223833r803642_rule STIG ID: RACF-TN-000040 Severity: CAT II

6.6.4 Ensure AT-TLS protection is enabled for the TN3270 Telnet Server (Manual)

Profile Applicability:

- Level 1

Description:

During the TLS handshake process, mutually acceptable suite of cryptographic algorithms is selected by the server and client. The algorithms specified in the selected suite are used to cryptographically protect the data that subsequently flows between the two. To apply TLS protection of adequate strength, the TN3270 Telnet server must be configured to use AT-TLS protection. Though the TN3270 Telnet server was initially implemented to use System SSL directly, that level of support no longer meets acceptable protection standards and is therefore not adequate. In z/OS V2R5, the native support for System SSL was removed from the TN3270 Telnet server.

Rationale:

Failure to properly enforce adequate encryption strength could result in the loss of data privacy.

Impact:

The cryptographic operations involved in TLS do come with a CPU cost. Most of the recommended algorithms are optimized using hardware acceleration. Depending on the number and frequency of TLS handshakes, the CPU impact could be noticeable.

Audit:

Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TN3270E Telnet server started task JCL. This file is often called the "Telnet profile." Check the following items are in effect for the configuration specified in the Telnet profile:

NOTE: If an `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

NOTE: FIPS 140-2 minimum encryption is the accepted level of encryption and will override this requirement if greater.

- Each `TELNETPARMS` block specifies the `TTLSPORT` statement, and the `PORT` statement is not used.
- The `TELNETPARMS CONNTYPE` statement is coded within each `TELNETPARMS` block with either the `SECURE`, `NEGTSECURE` or `NONE` value.

NOTE: The `CONNTYPE` statement can appear in both `TELNETPARMS` and `PARMSGROUP` statement blocks.

Use the `pasearch -t` command to check the AT-TLS policy rule(s) that are configured for each of the TN3270 server ports. While the specific requirements of each rule must accommodate the capabilities of the communication partners (the 3270 terminal emulators) that connect to the TN3270E server, you should strive for the use of strong protection. If possible, use settings that require the following:

- TLSv1.2 or a later version of the TLS protocol
- Cipher suites that use:
 - Ephemeral Diffie-Hellman key exchange (ECDHE (preferred) or DHE)
 - AES encryption (AES-GCM preferred)
 - SHA256 or stronger hashes

Remediation:

The system programmer will review the `TTLSPORT` and `TELNETPARMS CONNTYPE` statements and/or the `TELNETGLOBALS` statement in the Telnet profile. Ensuring that they conform to the requirements specified below.

Each `TELNETPARMS` block specifies the `TTLSEPORT` statement, and the `PORT` statement is not used.

The `TELNETPARMS CONNTYPE` statement is coded within each `TELNETPARMS` block with either the `SECURE`, `NEGTSECURE` or `NONE` value.

NOTE: The `CONNTYPE` statement can appear in both `TELNETPARMS` and `PARMSGROUP` statement blocks.

Use local procedures to configured AT-TLS policy rules for each of the TN3270E server ports. While the specific requirements of each rule must accommodate the capabilities of the communication partners (the 3270 terminal emulators) that connect to the server, you should strive for the use of strong protection. If possible, use settings that require the following:

- TLSv1.2 or a later version of the TLS protocol
- Cipher suites that use:
 - Ephemeral Diffie-Hellman key exchange exchange (ECDHE (preferred) or DHE)
 - AES encryption (AES-GCM preferred)
 - SHA256 or stronger hashes



Default Value:

No TLS protection is applied.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223831 Rule ID: SV-223831r604139_rule STIG ID: RACF-TN-000020 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |

6.6.5 Ensure SMF recording options for the TN3270 Telnet Server are configured (Manual)

Profile Applicability:

- Level 1

Description:

The TN3270 Telnet Server can provide audit data in the form of SMF records. The SMF data produced provides information about individual sessions. This data includes the VTAM application, the remote and local IP addresses, and the remote and local IP port numbers.

Rationale:

Failure to collect and retain audit data may contribute to the loss of accountability and hamper security audit activities.

Audit:

Refer to the Profile configuration file specified on the `PROFILE DD` statement in the TN3270E Telnet Server started task JCL. This file is often called the "Telnet profile." Ensure the following configuration statement settings are in effect in the Telnet profile configuration data set.

NOTE: If the `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

- The `TELNETPARMS SMFINIT` statement is coded with the TYPE119 operand within each `TELNETPARMS` statement block.
- The `TELNETPARMS SMFTERM` statement is coded with the TYPE119 operand within each `TELNETPARMS` statement block.

Remediation:

The system programmer responsible for the IBM Communications Server will review the `TELNETPARMS SMFINIT` and `SMFTERM` statements in the Telnet profile. Ensure they conform to the requirements specified below.

NOTE: If the `INCLUDE` statement is coded in the Telnet profile, the data set specified on this statement must be checked for the following items as well.

The `TELNETPARMS SMFINIT` statement is coded with the TYPE119 operand within each `TELNETPARMS` statement block.

The `TELNETPARMS SMFTERM` statement is coded with the TYPE119 operand within each `TELNETPARMS` statement block.






Default Value:

SMF recording of TN3270 events is disabled.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223759 Rule ID: SV-223759r604139_rule STIG ID: RACF-OS-000030 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v8 | 8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | |  |  |

6.6.6 Ensure Startup user account for the z/OS UNIX Telnet Server is defined (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS Unix Telnet Server (i.e., `otelnetd`) provides remote access to the z/OS Unix command prompt. `otelnetd` does not provide any cryptographic protection of user connections. Due to this lack of security, the `otelnetd` server will not be used. Instead, use SSH for remote z/OS Unix command prompt access.

Rationale:

The inability to cryptographically protect `otelnetd` connections exposes all communications between telnet clients and the `otelnetd` server, including sensitive values like passwords, to network-based observers, resulting in a complete lack of data privacy.

Impact:

`otelnetd` users (if any) will no longer have access to `otelnetd` and must switch to a secure remote access mechanism such as SSH.

Audit:

Ensure the following program controls are in effect for the `otelnetd` server:

1. Program resources `otelnetd` and `EZATNTLE` are defined to the `PROGRAM` resource class with a `UACC(NONE)`. The library name where these programs are located is `SYS1.TCPIP.SEZALOAD`.
2. No access to the program resources `otelnetd` or `EZATNTLE` is permitted.

Remediation:

Ensure that the `EZATNTLE` program and its alias `otelnetd` are defined to `RACF`, no access is granted, and `WARN` mode is not enabled. The following commands provide a sample of how this can be accomplished.

```
rdef program otelnetd addmem('sys1.tcpip.sezaload'//nopadchk) -  
data('Reference SRR PDI # IFTP0090') -  
audit(all(read)) uacc(none) owner(admin)  
rdef program ezatntle -  
addmem('sys1.tcpip.sezaload'//nopadchk) -  
data('Reference SRR PDI # IFTP0090') -  
audit(all(read)) uacc(none) owner(admin)
```

A `PROGRAM` class refresh will be necessary and can be accomplished with the command:

```
setr when(program) refresh
```



Default Value:

`otelnetd` is not enabled.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223864 Rule ID: SV-223864r604139_rule STIG ID: RACF-UT-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|---|---|
| v8 | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |

6.7 VTAM Recommendations

This section describes the VTAM recommendations.

6.7.1 Ensure VTAM USSTAB definitions are being used for secured terminals (Manual)

Profile Applicability:

- Level 1

Description:

VTAM options and definitions are used to define VTAM operational capabilities. They must be strictly controlled. Unauthorized users could override or change start options or network definitions.

Rationale:

Failure to properly control VTAM resources could potentially compromise the network operations.

Audit:

VTAM Systems Programmer supplies the following information:

- Documentation regarding terminal naming standards.
- Documentation of all procedures controlling terminal logons to the system.
- A complete list of all USS commands used by terminal users to log on to the system.
- Members and data set names containing `USSTAB` and `LOGAPPL` definitions of all terminals that can log on to the system (e.g., `SYS1.VTAMLST`).
- Members and data set names containing logon mode parameters.

Check that the `USSTAB` definitions are only used for secure terminals (e.g., terminals that are locally attached to the host or connected to the host via secure leased lines).

Remediation:

The Systems programmer will verify that `USSTAB` definitions are only used for secure terminals.

Only terminals that are locally attached to the host or connected to the host via secure leased lines located in a secured area. Only authorized personnel may enter the area where secure terminals are located.

`USSTAB` or `LOGAPPL` definitions are used to control logon from secure terminals. These terminals can log on directly to any VTAM application (e.g., TSO, CICS, etc.) of their choice and bypass Session Manager services. Secure terminals are usually locally attached to the host or connected to the host via a private LAN without access to an external network. Only authorized personnel may enter the area where secure terminals are located.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223870 Rule ID: SV-223870r604139_rule STIG ID: RACF-VT-000020 Severity: CAT II

6.7.2 Ensure System datasets used to support the VTAM network are secured (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Rationale:

Failure to properly control VTAM datasets could potentially compromise the network operations.

Audit:

- a) Create a list of data set names containing all VTAM start options, configuration lists, network resource definitions, commands, procedures, exit routines, all SMP/E TLIBs, and all SMP/E DLIBs used for installation and in development/production VTAM environments.
- b) Ensure that RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.

Remediation:

Ensure that RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.




The following sample RACF commands show proper definitions/permissions for VTAM datasets:

```
AD 'SYS1.VTAM*.*' UACC(NONE) OWNER(SYS1) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS1.VTAM*.*' ID() ACC(A)  
  
AD 'SYS1.VTAMLIB.*' UACC(NONE) OWNER(SYS1) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS1.VTAMLIB.*' ID() ACC(A)  
  
AD 'SYS1.VTAM.SISTCLIB.*' UACC(NONE) OWNER(SYS1) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS1.VTAM.SISTCLIB.*' ID() ACC(A)  
  
AD 'SYS3.VTAM.*' UACC(NONE) OWNER(SYS3) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('VTAM CUSTOMIZED DS: REF SRR PDI ZVTM0018')  
PE 'SYS3.VTAM.*' ID() ACC(A)  
  
AD 'SYS3.VTAMLIB.*' UACC(NONE) OWNER(SYS3) -  
AUDIT(SUCCESS(UPDATE) FAILURES(READ)) -  
DATA('IBM VTAM APF DS PROFILE: REF SRR PDI ZVTM0018')  
PE 'SYS3.VTAMLIB.*' ID() ACC(A)  
  
SETR GENERIC(DATASET) REFRESH
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223869 Rule ID: SV-223869r604139_rule STIG ID: RACF-VT-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7 Cryptography and Encryption

Integrated Cryptographic Service Facility - ICSF - is a software element of z/OS that works with hardware cryptographic features and the Security Server to provide secure, high-speed cryptographic services in the z/OS environment. ICSF provides the application programming interfaces by which applications request the cryptographic services. As such, the protection of ICSF's resources is critical to a secure system.

7.1 ICSF Installation and Configuration

Once ICSF has been installed on a z/OS system, there are a minimal set of configuration tasks that need to be performed to make ICSF operational. This section expands upon the set of post-installation configuration tasks to ensure the resources associated with ICSF have been protected.

7.1.1 Ensure that all ICSF Installation Datasets are protected. (Manual)

Profile Applicability:

- Level 1

Description:

The datasets installed by ICSF need to be protected from unauthorized modifications or deletions.

Rationale:

Integrated Crypto Service Facility (ICSF) can use privileged functions and/or have access to sensitive data. Failure to properly restrict access to their installed data sets could result in a loss of system integrity or customer data.

Audit:

The following datasets:

CSF.SCSFCLI0

CSF.SCSFHDRS

CSF.SCSFMOD0

CSF.SCSFMOD1

CSF.SCSFMSG0

CSF.SCSFOBJ

CSF.SCSFPNL0

CSF.SCSFSKL0

CSF.SCSFTLIB

Must have protection profiles with the following characteristics:

1. UACC(NONE)
2. No ID(*) on the access list
3. Not in WARNING mode
4. All accesses are being logged
5. READ access should be restricted to z/OS System Programmers or z/OS Security Administrators.

For each dataset in the list above, the following two RACF commands should be issued to determine which protection profiles are in place, and who has permission to those resources.

```
LD DA('<insert dataset name here>')
LD DA('<insert dataset name here>') GENERIC
```

For example:

```
ld da('ibmuser.test.list')
```

```
INFORMATION FOR DATASET IBMUSER.TEST.LIST

LEVEL   OWNER      UNIVERSAL ACCESS  WARNING  ERASE
-----  -
00      IBMUSER      NONE           NO       NO

AUDITING
-----
FAILURES (READ)

NOTIFY
-----
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----
ALTER        SYS1           NON-VSAM

GLOBALAUDIT
-----
NONE

VOLUMES ON WHICH DATASET RESIDES
-----
ISFUS1

NO INSTALLATION DATA
READY
```

Remediation:




Create protection profiles for each of the datasets in the list above with UACC (NONE). To create a protection profile in the DATASET class for a specific dataset and ensure the default permission is NONE, use the following command:

```
RDEFINE DATASET <insert dataset name here> UACC(NONE) AUDIT(ALL)
```

References:

1. z/OS ICSF for RACF Security Technical Implementation Guide :: Version 6, Release: 7 Benchmark Date: 27 Oct 2021
2. Vul ID: V-224513, Rule ID: SV-224513r520402_rule, STIG ID: ZICSR000, Severity: CAT II,

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.1.2 Ensure that the ICSF Started Task is protected (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be started via a started task. On z/OS, a started task should have a protection profile in the STARTED class that has neither the PRIVILEGED nor TRUSTED attribute, and the user ID identified in the STDATA field is neither UID(0) nor SPECIAL.

Rationale:

As a started task on a z/OS system, the ICSF started task must have a protection profile in the STARTED class to limit its abilities to impact other tasks running on the system. By ensuring the started task is neither TRUSTED nor PRIVILEGED, and ensuring the user ID associated with the started task is neither UID(0) nor SPECIAL, it ensures the ICSF address space is isolated from the rest.

Audit:

The ICSF started task must have a protection profile in the STARTED class that is neither TRUSTED nor PRIVILEGED.

The USER in the STDATA field for the protection profile should be neither UID(0) nor SPECIAL.

To find the name of the ICSF started task, use the command:

```
SEARCH CLASS(STARTED)
```

To identify the USER, TRUSTED, and PRIVILEGED attributes of the ICSF started task, use the command:

```
RLIST STARTED <ICSF started task name> STDATA
```

To determine if the user id UID(0) or SPECIAL, use the command:

```
LISTUSER <userid> OMVS
```

Remediation:

Create a protection profile in the STARTED class for the ICSF started task.

To create a protection profile in the DATASET class for a specific dataset and ensure the default permission is NONE, use the following command:




```
RDEFINE STARTED <ICSF started task name> UACC(NONE) STDATA(PRIVILEGED(NO)  
TRUSTED(NO) USER(<userid>)
```

To change the attributes of the user ID specified in the STDATA(USER(userid)) field, please see the RACF ALTUSER command.

References:

1. z/OS ICSF for RACF Security Technical Implementation Guide :: Version 6, Release: 7 Benchmark Date: 27 Oct 2021
2. Vul ID: V-224516, Rule ID: SV-224516r520411_rule, , STIG ID: ZICSR032, Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |

7.1.3 Ensure CSFINPV2 requires signature verification (Manual)

Profile Applicability:

- Level 1

Description:

Certain z/OS load modules can have an associated signature generated by IBM that is verified by the system when the module is loaded into system storage for execution. The way to ensure the signature verification occurs is by defining a profile in the PROGRAM class with the SIGVER segment.

Rationale:

By verifying the IBM generated signature when a module is loaded into storage, the integrity and authenticity of the module are guaranteed.

Audit:

The ICSF module CSFINPV2 must have a profile in the PROGRAM class with the SIGVER segments setup to require signature verification.

To determine that a protection profile for CSFINPV2 exists, and that it has the correct information in the SIGVER segment for module signing, enter the following command:

```
RLIST PROGRAM CSFINPV2 SIGVER
```

Remediation:

Create a protection profile in the STARTED class for the ICSF started task.

To create a protection profile in the PROGRAM class for module CSFINPV2, enter the following command.

```
RDEFINE PROGRAM CSFINPV2 ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ)
SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
```

And then refresh the PROGRAM class with the command:



```
SETROPTS WHEN(PROGRAM) REFRESH
```

Refer to the ICSF System Program's Guide for additional information.

Additional Information:

Refer to the ICSF System Programers's Guide for additional information.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. | |  |  |

7.1.4 Ensure ICSF is configured to start during IPL (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be started in different ways, including manual via a “START” operator command. To ensure maximum availability of ICSF and crypto services, it is best to configure ICSF to be started during the z/OS IPL procedures.

This can be done by configuring ICSF to start early as described in Chapter 4. "Operating ICSF", Section "Starting ICSF during IPL-time" in the ICSF System Programmer's Guide. The ICSF=xx parameter should be specified in IEASYSxx.

Rationale:

By configuring ICSF to start during IPL, there is less operator manual intervention required, and more availability of crypto services and resources.

Audit:

Ensure the IEASYSxx parmlib member has ICSFPROC and ICSF system parameters, e.g.:

```
ICSFPROC=CSF2  
ICSF=00
```

Ensure the ICSF started procedure has been modified to accept the PRM procedure variable, e.g.:

```
//CSF PROC PRM=00  
//CSF EXEC PGM=CSFINIT,REGION=0M,TIME=1440,MEMLIMIT=NOLIMIT  
//CSFPARM DD DSN=USER.PARMLIB(CSFPRM&PRM),DISP=SHR
```





Remediation:

Create the ICSFPROC and ICSF parameters in the IEASYSxx parmlib member and modify the ICSF started procedure to accept the PRM procedure variable.

Additional Information:

For more information, consult the “Starting ICSF during IPL-time” section in the [ICSF System Programmer's Guide](#).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |
| v8 | 3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. | |  |  |

7.2 ICSF Component Configuration

ICSF has a multitude of ways it can be configured to operate, most of them specified in a dataset member referred to as the “ICSF Installation Options Dataset”. This section outlines recommendations and requirements for ICSF configuration options with an emphasis on security.

7.2.1 Ensure Crypto Usage Statistics are enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be configured to capture statistics related to the use of cryptographic resources, for example key material, cryptographic hardware engines, or even specific cryptographic algorithms.

Rationale:

By employing ICSF Crypto Usage Statistics, it is possible to detect the use of crypto resources that are not recommended, such as weak algorithms.

Audit:

ICSF Crypto Usage Statistics are enabled via the `STATS` keyword in the ICSF Installation Options Dataset.

To determine the setting of the `STATS` keyword, issue the following command from an operation console and observe the value of the `STATS` keyword:

```
DISPLAY ICSF,OPTIONS
```

Eg:

```
STATS :  
SY1      ENG, SRV, ALG
```

Remediation:

Add the `STATS` keyword to the ICSF Installation Options Dataset and enter the following command at an operator console:

```
SETICSF OPTIONS, REFRESH
```

Optionally, the `STATS` parameter can be dynamically enabled by the following command:

```
SETICSF OPTIONS, STATS=(ENG, SRV, ALG)
```

Please note that if ICSF is restarted, the dynamic settings for the options will be reset to their definition in the ICSF Installation Options Dataset.




Default Value:

Crypto Usage Statistics are disabled.

Additional Information:

For more information, please see the “Parameters in the installation options dataset” section in the ICSF System Programmer’s Guide.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

7.2.2 Ensure Crypto Key Lifecycle Auditing is enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be configured to audit the lifecycle of key material, for example, key creation, key activation, key deletion, etc. The lifecycle events are recording using SMF Type 82 records.

Rationale:

By configuring ICSF to audit key lifecycle events, it is possible to preserve a record of all major events in a key's lifecycle.

Audit:

ICSF Crypto Lifecycle Auditing is enabled using the following keywords in the ICSF Installation Options Dataset.

AUDITKEYLIFECKDS

AUDITKEYLIFEKPDS

AUDITKEYLIFETKDS

To determine the setting of the key lifecycle auditing, issue the following command from an operation console and observe the value of the AUDITKEYLIFE*KDS keyword:

```
DISPLAY ICSF,OPTIONS
```

Eg:

```
AUDITKEYLIFECKDS: Audit CCA symmetric key lifecycle events
  SYSNAME  LABEL  TOKEN
  SY1      Yes    Yes
AUDITKEYLIFEKPDS: Audit CCA asymmetric key lifecycle events
  SYSNAME  LABEL  TOKEN
  SY1      Yes    Yes
AUDITKEYLIFETKDS: Audit PKCS #11 key lifecycle events
  SYSNAME  TOKOBJ  SESSOBJ
  SY1      No     No
```

Remediation:

Add the `AUDITKEYLIFECKDS`, `AUDITKEYLIFEPKDS`, or `AUDITKEYLIFETKDS` keywords to the ICSF Installation Options Dataset and enter the following command at an operator console:

```
SETICSF OPTIONS, REFRESH
```

Optionally, the key lifecycle auditing parameters can be dynamically enabled by the following commands:

```
SETICSF OPTIONS, AUDITKEYLIFECKDS, TOKEN=YES, LABEL=YES  
SETICSF OPTIONS, AUDITKEYLIFEPKDS, TOKEN=YES, LABEL=YES  
SETICSF OPTIONS, AUDITKEYLIFETKDS, TOKENOBJ=YES, SESSIONOBJ=YES
```

Please note that if ICSF is restarted, the dynamic settings for the options will be reset to their definition in the ICSF Installation Options Dataset.


Default Value:

ICSF Key Lifecycle Audit is disabled.

Additional Information:

For more information, please see the “Parameters in the installation options dataset” section in the ICSF System Programmer’s Guide.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|------|---|
| v8 | 3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal. | | |  |

7.2.3 Ensure Crypto Key Usage Auditing is enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF can be configured to audit the use of key material, whether or not the key material is stored in an ICSF key data set.

Rationale:

By configuring ICSF to audit key usage events, it is possible to document which users and/or jobs are using key material.

Audit:

ICSF Crypto Key Usage Auditing is enabled using the following keywords in the ICSF Installation Options Dataset.

AUDITKEYUSGCKDS

AUDITKEYUSGPKDS

AUDITKEYUSGTKDS

To determine the setting of the key usage auditing keywords, issue the following command from an operation console and observe the value of the AUDITKEYLIFE*KDS keyword:

```
DISPLAY ICSF,OPTIONS
```

Eg:

```
AUDITKEYUSGCKDS: Audit CCA symmetric key usage events
  SYSNAME  LABEL    TOKEN    Interval Days/HH.MM.SS
  SY1      Yes      Yes      000/01.00.00
AUDITKEYUSGPKDS: Audit CCA asymmetric key usage events
  SYSNAME  LABEL    TOKEN    Interval Days/HH.MM.SS
  SY1      Yes      Yes      000/01.00.00
AUDITPKCS11USG: Audit PKCS #11 usage events
  SYSNAME  TOKOBJ    SESSOBJ  NOKEY  Interval Days/HH.MM.SS
  SY1      No       No       No     001/00.00.00
```

Remediation:

Add the `AUDITKEYUSGCKDS`, `AUDITKEYUSGPKDS`, or `AUDITKEYUSGTKDS` keywords to the ICSF Installation Options Dataset and enter the following command at an operator console:

```
SETICSF OPTIONS,REFRESH
```

Optionally, the parameters can be dynamically enabled by the following commands:

```
SETICSF OPTIONS,AUDITKEYUSGCKDS,TOKEN=YES,LABEL=YES  
SETICSF OPTIONS,AUDITKEYUSGPKDS,TOKEN=YES,LABEL=YES  
SETICSF OPTIONS,AUDITPKCS11USG,TOKENOBJ=YES,SESSIONOBJ=YES
```

Please note that if ICSF is restarted, the dynamic settings for the options will be reset to their definition in the ICSF Installation Options Dataset.


Default Value:

ICSF Key Usage Audit is disabled.

Additional Information:

For more information, please see the “Parameters in the installation options dataset” section in the ICSF System Programmer’s Guide.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|------|---|
| v8 | 3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal. | | |  |

7.2.4 Ensure ICSF Key Data Sets have a system backup (Manual)

Profile Applicability:

- Level 1

Description:

ICSF stores key material in data sets known as “Key Data Sets”, KDS. Symmetric keys (AES, DES, HMAC) are stored in the CKDS, asymmetric keys (RSA, ECC, QSA) are stored in the PKDS, and PKCS#11 tokens and objects are stored in the TKDS. These datasets need to be included in an installation's backup procedure.

Rationale:

To prevent the permanent loss of key material, and thus the loss of encrypted data, ICSF's key data sets must be backed up according to installation procedures.

Audit:




Ensure all ICSF Key Data Sets are included in the system's backup procedure. The names of the Key Data Sets can be found by executing the following operator command:

```
DISPLAY ICSF,KDS
```

Remediation:

Add the ICSF Key Data Sets to the system's backup procedure.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 11.2 Perform Automated Backups Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. |  |  |  |

7.2.5 Ensure ICSF Master Keys have a backup procedure (Manual)

Profile Applicability:

- Level 1

Description:

In the context of ICSF, a “master key” is a key that is loaded and stored on a Crypto Express Coprocessor, whether configured in CCA mode or EP11 mode. This master key is used to encipher key material when it exists outside the boundary of the CEX coprocessor, and thus is required to make the key material usable. It is critical that the master key values can be recovered if needed.

Rationale:

ICSF’s operational keys are enciphered using the Crypto Express master key, thus if the master key is lost or damaged, the key material stored in ICSF Key Data Sets are not usable. It is critical that the master key values be backed up such that if needed, the master key registered on the Crypto Express Coprocessor can be restored to their correct values so operational keys in ICSF can continue to be used.

Audit:

Ensure there is a procedure in place to backup the values of the master keys installed on the Crypto Express Coprocessors active on the system. To see what master keys are active, enter the following operator command:

```
DISPLAY ICSF,MKS
```

Eg:




| FEATURE | SERIAL# | STATUS | AES | DES | ECC | RSA | P11 |
|---------|----------|--------|-----|-----|-----|-----|-----|
| 7C00 | 99EA6055 | Active | A | A | A | A | |

In the above case, the AES, DES, ECC, and RSA master keys are active and must be part of backup procedure. The Enterprise PKCS#11 master key is not active.

Remediation:

Create a procedure for backing up and restoring the Crypto Express master keys.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

7.2.6 Ensure all ICSF Key Data Sets are in Common Record Format (Manual)

Profile Applicability:

- Level 1

Description:

The format of ICSF Key Data Sets have evolved over time. The most recent format, referred to as “Common Record Format” or KDSR, is recommended as it enables features such as key reference date tracking.

Rationale:

The ICSF Key Data Sets must be in KDSR format in order to enable advanced security features such as key reference date tracking.

Audit:

To discover the format of each ICSF KDS, enter the following operator command:

```
DISPLAY ICSF,KDS
```

Eg:

```
CKDS  ISFTEST.BPETTI.CKDS.KDSRL
      FORMAT=KDSRL          SYSPLEX=N  MKVPs=DES AES
      DES MKVP date=Unknown
      AES MKVP date=Unknown
PKDS  ISFTEST.BPETTI.PKDS.KDSRL
      FORMAT=KDSRL          SYSPLEX=N  MKVPs=RSA ECC
      RSA MKVP date=Unknown
      ECC MKVP date=Unknown
TKDS  ISFTEST.BPETTI.TKDS.KDSR2
      FORMAT=KDSRL          SYSPLEX=N  MKVPs=P11 RCS
      P11 MKVP date=Unknown
```

In the above example, all KDS are in KDSRL (KDSR “long”) format, which allows the enabling of features like key reference date tracking.

Remediation:

To convert a key data set to common record format using the ICSF panels, do the following:

1. On the ICSF Primary Menu panel, select option 2, `KDS MANAGEMENT` and press `ENTER`.
2. When the ICSF Key Data Set Management panel appears, select the type of key data set you want to convert and press `ENTER`.
3. On the next panel, select the `COORDINATED xKDS CONVERSION` option and press `ENTER`.
4. When the ICSF Coordinated KDS conversion panel appears, fill in the required fields and press `ENTER`.

Additional Information:

For more information, please see the “Converting a key data set to common record format” section in the [ICSF Administrator’s Guide](#).

7.2.7 Ensure all ICSF Key Data Sets are enabled for sysplex sharing (Manual)

Profile Applicability:

- Level 1

Description:

For ICSF to share key material across a sysplex, the ICSF Installation Options Dataset must contain the following keywords.

SYSPLEXCKDS

SYSPLEXPKDS

SYSPLEXTKDS

Rationale:

When the ICSF Key Datasets are shared among members of a sysplex, it is critical that updates to the data sets are communicated across all members of the sysplex group. To enable the sysplex communication, the ICSF Installation Options Dataset must contain the appropriate sysplex enablement keywords.

Audit:

To determine the `sysplex` settings for each ICSF Key Data Set, use the Installation Option Display `ISPF` utility.

From the ICSF Primary Menu panel, select option 3 `OPSTAT`.

From the ICSF Installation Options panel, select option 1 `OPTIONS`

The `sysplex` settings for the ICSF Key Datasets are shown as for example:

| | | |
|-------------|--------------------------------------|--------------|
| SYSPLEXCKDS | Sysplex consistency for CKDS updates | NO, FAIL(NO) |
| SYSPLEXPKDS | Sysplex consistency for PKDS updates | NO, FAIL(NO) |
| SYSPLEXTKDS | Sysplex consistency for TKDS updates | NO, FAIL(NO) |

Remediation:

There is no dynamic activation for the KDS `sysplex` keywords in the installation options dataset. To enable `sysplex` communication, add the following keywords to the ICSF Installation Options Dataset and stop/restart ICSF.

```
SYSPLEXCKDS (YES, FAIL (YES) )  
SYSPLEXPKDS (YES, FAIL (YES) )  
SYSPLEXTKDS (YES, FAIL (YES) )
```

Default Value:

The default is SYSPLEXCKDS(NO,FAIL(NO)) SYSPLEXPKDS(NO,FAIL(NO))
SYSPLEXTKDS(NO,FAIL(NO))

Additional Information:

For more information, please see the “Parameters in the installation options data set” section in the ICSF Programmer’s Guide.

7.2.8 Ensure ICSF is running with FIPSMODE enabled (Manual)

Profile Applicability:

- Level 1

Description:

If FIPSMODE(YES) is specified in the ICSF Installation Options Dataset, the PKCS#11 services that ICSF provides will operate in compliance with Federal Information Processing Standard Security Requirements for Cryptographic Modules, referred to as FIPS 140-2.

Rationale:

By operating in compliance with FIPS 140-2, ICSF's PKCS#11 services will ensure the use of strong keys and FIPS 140-2 approved encryption algorithms.

Audit:

To determine the `sysplex` settings for each ICSF Key Data Set, use the Installation Option Display `ISPF` utility.

From the ICSF Primary Menu panel, select option 3 `OPSTAT`.

From the ICSF Installation Options panel, select option 1 `OPTIONS`

The `FIPSMODE` setting is shown as for example:

| | | |
|----------|-------------------------------------|--------------|
| FIPSMODE | Operate PKCS #11 in FIPS 140-2 mode | NO, FAIL(NO) |
|----------|-------------------------------------|--------------|

Remediation:

Add the following keywords to the ICSF Installation Options Dataset and stop/restart ICSF:

| |
|-----------------------------|
| FIPSMODE (YES, FAIL (YES)) |
|-----------------------------|

Default Value:



The default is:

| |
|---------------------------|
| FIPSMODE (NO, FAIL (NO)) |
|---------------------------|

Additional Information:

For more information, please see the "Parameters in the installation options data set" section in the ICSF Programmer's Guide.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | |  |  |

7.2.9 Ensure CCA Operational Keys Are Created with WRAPENH3 Key Wrapping (Manual)

Profile Applicability:

- Level 1

Description:

When the Crypto Express Coprocessor is configured to run in CCA mode, keys generated by the coprocessor are enciphered using the coprocessor's master key (e.g. DES keys are enciphered by the DES master key). The way the keys are enciphered by the master key is referred to as the wrapping method. The most recent wrapping method, WRAPENH3, provides the first proprietary TDES key token (also known as a key block) to be independently reviewed and confirmed to be compliant with Payment Card Industry (PCI) Security Standard Council (SSC) PIN Security key block requirements as updated Sep 30, 2020.

Rationale:

Creating DES keys using WRAPENH3 will ensure those key blocks are PCI compliant as noted above.

Audit:

The wrapping method used by default for creating CCA keys is specified in the installation options dataset using the `DEFAULTWRAP` keyword. To determine the current value, use the ICSF panel utilities:

From the ICSF Primary Menu panel, select option 3 `OPSTAT`.

From the ICSF Installation Options panel, select option 1 `OPTIONS`

The `DEFAULTWRAP` setting is shown as for example:

| | | |
|--------------------------|---|-----------------------|
| <code>DEFAULTWRAP</code> | Default symmetric key wrapping - internal | <code>ORIGINAL</code> |
| <code>DEFAULTWRAP</code> | Default symmetric key wrapping - external | <code>ORIGINAL</code> |

Remediation:

Add the following keywords to the ICSF Installation Options Dataset and stop/restart ICSF:

| |
|---|
| <code>DEFAULTWRAP (WRAPENH3, WRAPENH3)</code> |
|---|



Default Value:

| |
|---|
| <code>DEFAULTWRAP (ORIGINAL, ORIGINAL)</code> |
|---|

Additional Information:

For more information, please see the "Parameters in the installation options data set" section in the ICSF Programmer's Guide.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | 3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. | |  |  |

7.3 ICSF Security Configuration

ICSF offers many resources and services to users which can be protected using various RACF classes and resource profiles. This section provides recommendations for securing the ICSF resources

7.3.1 Ensure CSFSERV class is active (Manual)

Profile Applicability:

- Level 1

Description:

The CSFSERV SAF class is used to protect access to ICSF callable services and utilities.

Rationale:

Users can be permitted or restricted from using ICSF callable services and utilities by enabling profiles within the CSFSERV class.

Audit:

The `SETROPTS LIST` command is used to identify which classes are active on the system. Execute a `SETROPTS LIST` command from a TSO session and search for the CSFSERV class.

If the class is active, check the universal access to the resources within that class by executing the following commands from a TSO session:

```
SEARCH CLASS(CSFSERV)
```

And for each profile returned

```
RLIST CSFSERV <profile name>
```

And examine the `Universal Access` setting. If the `Universal Access` setting is other than `NONE`, consult with your security administrator for the proper value.

Remediation:

Activate the CSFSERV class by issuing the following command from a TSO session:

```
SETR CLASSACT(CSFSERV) RACLIST(CSFSERV)
```




For resources that require an update to `UACC(NONE)`, execute the following command from a TSO session:

```
RALTER CSFSERV <profile name> UACC(NONE)
```

Default Value:

The CSFSERV class is not active.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.3.2 Ensure CSFKEYS class is active (Manual)

Profile Applicability:

- Level 1

Description:

The CSFKEYS SAF class is used to protect access to key material stored in an ICSF Key Data Set.

Rationale:

Users can be permitted or restricted from access key material by enabling profiles within the CSFSERV class.

Audit:

The `SETROPTS LIST` command is used to identify which classes are active on the system. Execute a `SETROPTS LIST` command from a TSO session and search for the CSFKEYS class.

If the class is active, check the universal access to the resources within that class by executing the following commands from a TSO session:

```
SEARCH CLASS(CSFKEYS)
```

And for each profile returned

```
RLIST CSFKEYS <profile name>
```

And examine the Universal Access setting. If the Universal Access setting is other than NONE, consult with your security administrator for the proper value.

Remediation:

Activate the CSFKEYS class by issuing the following command from a TSO session:

```
SETR CLASSACT(CSFKEYS) RACLIST(CSFSERV)
```




For resources that require an update to UACC(NONE), execute the following command from a TSO session:

```
RALTER CSFKEYS <profile name> UACC(NONE)
```

Default Value:

The CSFKEYS class is not active.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.3.3 Ensure CRYPTOZ class is active (Manual)

Profile Applicability:

- Level 1

Description:

The CRYPTOZ class is used to protect tokens and objects stored in the ICSF Token Data Set (TKDS).

Rationale:

Users can be permitted or restricted from access tokens and objects in the TKDS by using resource profiles the CRYPTOZ class.

Audit:

The SETROPTS LIST command is used to identify which classes are active on the system. Execute a SETROPTS LIST command from a TSO session and search for the CRYPTOZ class.

If the class is active, check the universal access to the resources within that class by executing the following commands from a TSO session:

```
SEARCH CLASS(CRYPTOZ)
```

And for each profile returned

```
RLIST CRYPTOZ <profile name>
```

And examine the Universal Access setting. If the Universal Access setting is other than NONE, consult with your security administrator for the proper value.

Remediation:

Activate the CRYPTOZ class by issuing the following command from a TSO session:

```
SETR CLASSACT(CRYPTOZ) RACLIST(CRYPTOZ)
```




For resources that require an update to UACC(NONE), execute the following command from a TSO session:

```
RALTER CRYPTOZ <profile name> UACC(NONE)
```

Default Value:

The CRYPTOZ class is not active.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.3.4 Ensure the XCSFKEY class is active (Manual)

Profile Applicability:

- Level 1

Description:

While the `CSFKEYS` class controls who has access to key material, the `XCSFKEY` class provides additional controls regarding how the keys can be used. For example, it is possible to setup profiles in the `XCSFKEY` class to restrict a key's ability to be used as an exporter or importer key.

Rationale:

The `XCSFKEY` class provides usage control in addition to access permission provided by the `CSFKEYS` class.

Audit:

The `SETROPTS LIST` command is used to identify which classes are active on the system. Execute a `SETROPTS LIST` command from a `TSO` session and search for the `XCSFKEY` class.

Remediation:




Activate the `XCSFKEY` class by issuing the following command from a `TSO` session:

```
SETR CLASSACT(XCSFKEY) RACLIST(CRYPTOZ)
```

Default Value:

The `XCSFKEY` class is not active.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.3.5 Ensure ICSF Key Store Policy controls are enabled (Manual)

Profile Applicability:

- Level 1

Description:

ICSF Key Store Policy governs the use of key tokens in callable services. A key token is just a control block of key material that can be passed directly as an input parameter to an ICSF callable service – as opposed to specifying the label of a key stored in an ICSF Key Data Set. The Key Store Policy settings control how permission to use a key token is performed.

Rationale:

The ICSF Key Store Policy controls make it possible to provide protection profiles to key tokens in addition to key labels.

Audit:

First, the `XFACILITY` class has to be active. Execute a `SETROPTS LIST` command from a `TSO` session and search for the `XCSFKEY` class.

Second, ensure the following resources are defined in the `XFACILIT` class

```
CSF.CKDS.TOKEN.CHECK.LABEL.FAIL
CSF.PKDS.TOKEN.CHECK.LABEL.FAIL
```

Issue the following command to determine what profiles exist in the `XFACILIT` class:

```
SEARCH CLASS(XFACILIT)
```

Remediation:

Activate the `XFACILIT` class by issuing the following command from a `TSO` session:

```
SETR CLASSACT(XFACILIT) RACLIST(CRYPTOZ)
```

Define the Key Store Policy controls within the `XFACILIT` class

```
RDEF XFACILIT CSF.CKDS.TOKEN.CHECK.LABEL.FAIL
RDEF XFACILIT CSF.PKDS.TOKEN.CHECK.LABEL.FAIL
```




Default Value:

The `XFACILIT` class is not active.

Additional Information:

For more information in ICSF's Key Store Policy controls, see the section "Maintaining Cryptographic Keys" with subsection "Key Store Policy" in the [ICSF Administrator's Guide](#).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | <u>3.3 Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.3.6 Ensure ICSF Key Datasets are protected (Manual)

Profile Applicability:

- Level 1

Description:

ICSF has three key data sets (KDS) which are used to store cryptographic keys for application use. The three are the CKDS for CCA symmetric keys (AES, DES, HMAC), the PKDS for CCA asymmetric keys (RSA, ECC, QSA), and the TKDS for PKCS#11 tokens and key objects. These key data sets need to be protected to avoid damage or destruction to critical key material.

Rationale:

The ICSF key data sets are critical to the system and a RACF profile in the DATASET class is required to ensure no malicious or inadvertent damage can occur.

Audit:

It should be noted that multiple key data sets of each type can exist on the system, but only one of each can be active at any point in time. All key data sets need protection, but ICSF only knows the name of the active KDS.

To find the name of the active KDS, enter the following operator command:

```
DISPLAY ICSF,KDS
```

The names of the active KDS will be shown in the resulting output messages.

```
CKDS  ISFTEST.BPETTI.CKDS.KDSRL
      FORMAT=KDSRL          SYSPLEX=N  MKVPs=DES AES
      DES MKVP date=Unknown
      AES MKVP date=Unknown
PKDS  ISFTEST.BPETTI.PKDS.KDSRL
      FORMAT=KDSRL          SYSPLEX=N  MKVPs=RSA ECC
      RSA MKVP date=Unknown
      ECC MKVP date=Unknown
TKDS  ISFTEST.BPETTI.TKDS.KDSR2
      FORMAT=KDSRL          SYSPLEX=N  MKVPs=P11 RCS
      P11 MKVP date=Unknown
```

Once the names of the KDS have been determined, the existence of a profile in the DATASET class can be demonstrated by issuing the following command from a TSO session:

```
LA DA('<insert key data set name here>')
```

Remediation:




To create a profile in the `DATASET` class for each `KDS`, enter the following command:

```
RDEFINE DATASET <insert KDS name here> UACC(NONE)
```

Additional Information:

For more information on ICSF's key data sets, please see "Chapter 4. Setting up and maintaining cryptographic key data sets" in the [ICSF Administrator's Guide](#).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

7.3.7 Ensure ICSF administrative services are protected (Manual)

Profile Applicability:

- Level 1

Description:

ICSF has an extensive ISPF panel architecture which can be used to administer ICSF and its resources. The use of these panels should be restricted from unauthorized use.

Rationale:

Since the ICSF ISPF panels can control ICSF resources and ICSF operating characteristics, it is critical that only authorized users have access to these panels to avoid outages or resource corruption.

Audit:

Access to ICSF ISPF panels are governed by profiles in the CSFSERV class. To determine which profiles exist, enter the following command at a TSO session:

```
SEARCH CLASS(CSFSERV)
```

The following administrative services should be included in the search output:

```
CSFBRCK CKDS Key Utility
CSFBRPK PKDS Key Utility
CSFBRTK TKDS Browser
CSFCMK Change Master Key Utility
CSFCONF PCF CKDS to ICSF CKDS conversion utility
CSFCRC Coordinated KDS Administration
CSFDKCS Master Key Entry Utility
CSFGKF Generate Fingerprint Utility
CSFGGUP Key Generator Utility Program
CSFOPKL Operational Key Load
CSFPCAD Cryptographic Processor Management (active/deactivate)
CSFPKDR PKDS Reencipher and Refresh
CSFPMCI Pass Phrase Initialization
CSFREFR CKDS or PKDS Refresh
CSFRSWS Administrator Control Functions Utility (enable)
CSFRWP CKDS Conversion2 Utility - Rewrap
CSFSMK Set Master Key
CSFSSWS Administrative Control Functions Utility (disable)
CSFUDM User Defined Extensions (UDX) management functions
```

Remediation:




If any of the profiles listed above are missing in the `SEARCH CLASS(CSFSESV)` output, the following command can be used to define a profile.

```
RDEFINE CSFSESV <CSFxxxx Service Name> UACC(NONE)
```

Additional Information:

For more information on these administrative utilities and their protection resources, please see “Chapter 5: Controlling who can use cryptographic keys and services” in the [ICSF Administrator's Guide](#).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |

7.3.8 Ensure ICSF operator commands are protected (Manual)

Profile Applicability:

- Level 1

Description:

ICSF has two commands that can be issued at an operator console to display information about ICSF and ICSF resources or make changes to how ICSF is operating:

```
DISPLAY ICSF
```

```
SETICSF
```

Rationale:

Use of the ICSF operator commands must be restricted to authorized users.

Audit:

ICSF uses the following resource names to control access to the ICSF operator commands:

```
MVS.DISPLAY.ICSF
```

```
MVS.SETICSF.ICSF
```

To see if there are protection profiles for these resources, execute the following command:

```
SEARCH CLASS (OPERCMDS)
```

And scan the output for the above ICSF resource names.

For each of the resources, the following command can be used to determine the default access (UACC).

```
RLIST OPERCMDs <profile name>
```

_NOTE: Many installations will have a generic profile in place for display commands with more broad access allowed. _

Remediation:




For each of the ICSF operator command resource names, create a profile in the OPERCMDs class with permissions as defined by your security administrator

```
RDEFINE OPERCMDs <ICSF Operator Command Resource Name> UACC(NONE)
```

Additional Information:

For more information on these operator commands, please see the section “ICSF Operator Commands” in the ICSF System Programmer’s Guide.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | <u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |

8 Job Management JES2

This section describes the Job Management JES2 recommendations.

8.1 JES2 Commands

This section describes the JES2 Commands recommendations.

8.1.1 Ensure that JES2 system commands are protected (Manual)

Profile Applicability:

- Level 1

Description:

JES2 system commands are used to control JES2 resources and the operating system environment. Failure to properly control access to JES2 system commands could result in unauthorized personnel issuing sensitive JES2 commands.

Rationale:

If commands are not protected, this may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data. While JES2 operator commands cannot directly access sensitive data, it could change the routing of data such that it is available in an inappropriate environment.

Audit:

The `JES2.**` resource must be defined to the OPERCMDS class with a default access of `NONE` and with resource defined so that the security product logs all access. Access to JES2 system commands must be restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

Remediation:

Extended MCS support allows the installation to control the use of JES2 system commands through RACF. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

To control access to JES2 system commands, apply the following recommendations when implementing security:




1. Define the JES2.** resource in the OPERCMDS class with a default access of NONE and defined so that the security product logs all access.
2. Define specific JES2 system commands to RACF and restrict access to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

```
RDEFINE OPERCMDS JES2.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
PERMIT JES2.** CL(OPERCMDS) ID(SYSOPER) ACC(UPDATE)  
SETROPTS RACL(OPERCMDS) REF
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223754 Rule ID: SV-223754r604139_rule STIG ID: RACF-JS-000100 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.2 JES2 SPOOL

This section describes the JES2 SPOOL recommendations.

8.2.1 Ensure that JESSPOOL CLASS is active (Manual)

Profile Applicability:

- Level 1

Description:

JESSPOOL resources controls access to data stored on the JES SPOOL data sets. This includes all SYSOUT and instream data set, JCL, SYSLOG, JESTRACE, and JESNEWS data sets stored on spool and the control blocks that represent those data set. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing user ID and password information.

Rationale:

If the JESSPOOL class is not active, the integrity and availability of the operating system environment is compromised, and potentially sensitive customer data is exposed. Failure to set the JESSPOOL class active and properly protect the resources covered by the JESSPOOL class could allow access to any data stored on the JES spool.

Audit:

Ensure that the JESSPOOL resource class is active

Remediation:

Ensure that the JESSPOOL resource class is active:
Use RACF Command:

```
SETROPTS CLASSACT(JESSPOOL) .
```

Note that you should also enable `GENERIC` and optionally `RACLIST` this class in memory.

```
SETROPTS GENERIC(JESSPOOL) GENCMD(JESSPOOL)  
SETROPTS RACLIST(JESSPOOL)
```

Resources in the `JESSPOOL` class are not required for a user to access data that they own or a SYSOUT data set that is destined to the user (via the `WRITER=` or `DEST=`).

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223750 Rule ID: SV-223750r604139_rule STIG ID: RACF-JS-000060 Severity: CAT II

8.2.2 *Ensure that JES2 spool resources are protected (Manual)*

Profile Applicability:

- Level 1

Description:

JESSPOOL resources controls access to data stored on the JES SPOOL data sets. This includes all SYSOUT and instream data set, JCL, SYSLOG, JESTRACE, and JESNEWS data sets stored on spool and the control blocks that represent those data set. Failure to properly control JES2 spool resources could result in unauthorized personnel accessing job output, system activity logs, and trace data containing user ID and password information. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Failure to manager access to resources in the JESSPOOL class may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data. Failure to set the JESSPOOL class active and properly protect the resources covered by the JESSPOOL class could allow access to any data stored on the JES spool.

Audit:

Verify that the accesses to the JESSPOOL resources are properly restricted. Resources in the JESSPOOL class are not required for a user to access data that they own or a SYSOUT data set that is destined to the user (via the `WRITER=` or `DEST=`). Review the JESSPOOL report for resource permissions with the following naming convention. These profiles may be fully qualified, be specified as generic, or be specified with masking as indicated below:

| |
|---|
| <code>localnodeid.userid.jobname.jobid.dsnumber.name</code> |
|---|

localnodeid The name of the NJE node on which the SYSIN or SYSOUT data set currently resides.

userid The user ID associated with the job (or data set). This is the user ID RACF uses for validation purposes when the job runs (or the SYSOUT is created).

jobname The name that appears in the name field of the JOB statement.

jobid The job number JES2 assigned to the job.

dsnumber The unique data set number JES2 assigned to the spool data set. A “D” is the first character of this qualifier.

name The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify `DSN=` on the DD statement that creates the spool data set, JES2 uses a question mark (?).

Additional special purpose JESSPOOL resources:

- `Localnodeid.userid.SYSLOG.SYSTEM.sysname` is used to protect the logical SYSLOG data set associated with the system sysname. The user ID is generally set to “+MASTER+”.
- `Localnodeid.userid.jobname.jobid.jes_dsname` is used to protect certain specific JES data sets associated with a job. `jes_dsname_` is one of `EVENTLOG`, `JCL`, `JESJCL`, `JESMSGLG`, or `JESYSMSG`.

All users have access to their own JESSPOOL resources without the need for profiles in the JESSPOOL class.

The *localnodeid.* resource will be restricted to only system programmers, operators, and automated operations personnel with access of ALTER. All access will be logged.

(*localnodeid.* resource includes all generic and/or masked permissions, example: *localnodeid.***, *localnodeid.**, etc).

The JESSPOOL *localnodeid.userid.jobname.jobid.dsnumber.name*, whether generic and/or masked, can be made available to users, when approved by the IAO. Access will be identified at the minimum access for the user to accomplish the users function.

UPDATE, CONTROL, and ALTER access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes.

Remediation:

The JESSPOOL resources may be fully qualified, be specified as generic, or be specified with masking as indicated above.

By default, a user has access only to that user's own JESSPOOL resources. However, situations exist where a user legitimately requires access to jobs that run under another user's user ID. In particular, if a user routes SYSOUT to an external writer, the external writer should have access to that user's SYSOUT.

The `localnodeid. resource` will be restricted to only system programmers, operators, and automated operations personnel with access of ALTER. All access will be logged. (`localnodeid. resource` includes all generic and/or masked permissions, example: `localnodeid.**`, `localnodeid.*`, etc)

```
RDEF JESSPOOL localnodeid.** UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('PROTECT JESSPOOL AT HIGH LEVEL')
PE localnodeid.** CL(JESSPOOL) ID(syspau dt) ACC(A)
```

The JESSPOOL `localnodeid.userid.jobname.jobid.dsnumber.name`, whether generic and/or masked, can be made available to users, when approved by the IAO. Access will be identified at the minimum access for the user to accomplish the users function, SERVICE(READ, UPDATE, DELETE, ADD). All access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes. If frequent situations occur where users working on a common project require selective access to each other's jobs, then the installation may delegate to the individual users the authority to grant access, but only with the approval of the IAO.




```
RDEF JESSPOOL localnode.userid.jobname.jobid.dsnumber.name -
UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) -
DATA('PROTECT JESSPOOL')
PE _localnode.userid.jobname.jobid.dsnumber.name_ CL(JESSPOOL) ID() ACC(R)
```

If IBM's SDSF product is installed on the system, resources defined to the JESSPOOL resource class control functions related to jobs, output groups, and SYSIN/SYSOUT data sets on various SDSF panels.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223753 Rule ID: SV-223753r604139_rule STIG ID: RACF-JS-000090 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.2.3 Ensure that JES2 trace resources are protected (Manual)

Profile Applicability:

- Level 1

Description:

The JES2 tracing facility can be used to diagnose various problems that can occur in JES2. The data being logged may contain sensitive data and could include:

- Data from instream data set
- Data from SYSOUT data sets with PI data
- JCL statements including JOB cards potentially with passwords
- NJE headers including JOB headers potentially with passwords SYSOUT containing this trace data is associated with the \$TRCLOG job and is protected by resources in the JESSPOOL class. Failure to protect this resource may compromise the confidentiality of customer data.

Rationale:

Since all trace data is intended to diagnose problems with how the system manages data, there are cases where that data may contain sensitive information. All trace diagnostic data should be treated as if it contains sensitive data and protected from unauthorized access.

Audit:

Review the following resources defined to the JESSPOOL resource class:

```
localnodeid.jesid.$TRCLOG.jobid.dsnumber.JESTRACE
```

NOTE: These resource profiles may be more generic as long as they pertain directly to the JESTRACE data sets. For example:

```
localnodeid.jesid.$TRCLOG.*.*.JESTRACE
```

NOTE: Review the JES2 parameters to determine the localnodeid by searching for OWNNODE in the NJEDEF statement, and then searching for NODE (nnnn) (where nnnn is the value specified by OWNNODE). The NAME parameter value specified on this NODE statement is the localnodeid.

Another method is to issue the JES2 command \$D NODE,NAME,OWNNODE=YES to obtain the NAME of the OWNNODE.

Ensure that access authorization for the resources mentioned above is restricted to Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems.

Remediation:

Ensure the following resources are defined to the JESSPOOL resource class with a UACC (NONE) :

```
localnodeid.jesid.$TRCLOG.jobid.*.JESTRACE
```

Where `localnodeid` is the local NJE node, `jesid` is the user ID assigned to the JES2 address space, and `jobid` is the jobid of the \$TRCLOG job.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223752 Rule ID: SV-223752r767089_rule STIG ID: RACF-JS-000080 Severity: CAT II

8.2.4 Ensure that JESNEWS resources are protected (Manual)

Profile Applicability:

- Level 1

Description:

JESNEWS is a spool data set that is added after the job separator when SYSOUT is printed. Installation use this facility to communicate information to their user community. Ensure that access authorization for updating JESNEWS is restricted to appropriate personnel (i.e., users responsible for maintaining the JES News data set).

Printing the JESNEWS spool data set requires that the owner of the SPOOL data set being printed have access to the JESSPOOL profile protected the JESSPOOL data set.

Rationale:

JESNEWS is intended to print information to a wide group of users of the system. The ability to create or delete a JESNEWS data set should be limited to system personnel.

Audit:

Audit Procedure:

Ensure the following items are in effect:

- The `jesname.UPDATE.JESNEWS` resource is defined to the `OPERCMD` resource class with a default access of `NONE` and all access is logged.
NOTE: `jesname` is typically the name of the JES2 subsystem. Refer to the `SUBSYS` report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The `SUBSYSTEM NAME` of this entry is the name of the JES2 subsystem.
- Access authorization to the `jesname.UPDATE.JESNEWS` resource in the `OPERCMD` class restricts `CONTROL` access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.
Printing the JESNEWS spool data set requires that the owner of the SPOOL data set being printed have `READ` access to the JESSPOOL profile

```
localnodeid.jesid.$JESNEWS.jobid.dsnumber.JESNEWS
```

NOTE: These resource profiles may be more generic as long as they pertain directly to the JESNEWS data sets. For example:

```
localnodeid.jesid.$JESNEWS.*.*.JESNEWS
```

If JESNEWS is being used, a UACC of `READ` is used for the JESSPOOL resource controlling access to the JESNEWS data set.

Remediation:

Ensure the following items are in effect:

1. The `jesname.UPDATE.JESNEWS` resource is defined to the OPERCMDS resource class with a default access of NONE and all access is logged.
NOTE: `jesname` is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.
2. Access authorization to the `jesname.UPDATE.JESNEWS` resource in the OPERCMDS class restricts CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.




Examples of setting up proper protection are shown here:

```
RDEF OPERCMDS JES2.UPDATE.JESNEWS UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('MANAGE JESNEWS FUNCTION')  
PERMIT JES2.UPDATE.JESNEWS CLASS(OPERCMDS) ID() ACCESS(CONTROL)
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223751 Rule ID: SV-223751r604139_rule STIG ID: RACF-JS-000070 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3 Job Level Protection

This section describes the Job Level Protection recommendations.

8.3.1 Ensure that JESJOBS CLASS is set up (Manual)

Profile Applicability:

- Level 1

Description:

The JESJOBS class controls access to job level resources. The high-level qualifier for entities in this class are used to specify which functions are being controlled. When defining resources in the JESJOBS class, avoid generic high-level qualifiers such as '*' as these could have impacts beyond the original intended purpose (especially as new resources are added to the class).

Rationale:

The JESJOBS class is used to control actions against jobs and the ability to access job related data. These types of actions and access should be restricted to appropriate personnel. Actions could be performed by unauthorized personnel that would disrupt normal processing.

Audit:

Examine the resources in the JESJOBS class. In particular, look for backstop profiles that apply to multiple high-level qualifiers that grant access to all users (UACC) or inappropriate individual users.

The following lists the various high-level qualifiers:

| High level qualifier | Resource managed |
|----------------------|--|
| CANCEL | Cancel a job via the TSO cancel command or the job modify SSI |
| ENCRYPT | Provide a key label to use to encrypt SPOOL data sets for a job |
| GROUPREG | Controls added jobs to a JOBGROUP |
| HOLD | Hold a job via the job modify SSI |
| JOBCLASS | Controls access to a job group (enabled using FACILITY class profiles) |
| JOBNFY | Control who can use HTTP post notification of job status |
| updated | |
| MODIFY | Modify a job attributes via the job modify SSI |
| PURGE | Purge a job via the job modify SSI |
| RELEASE | Release (un-hold) a job via the job modify SSI |
| REROUTE | Reroute a job's NJE execution node via the job modify SSI |
| SPIN | Spin SYSOUT data sets via the job modify SSI |
| SPOOLIO | Read job level control blocks from SPOOL |
| START | Start a job immediately (\$S job) via the job modify SSI |
| SUBMIT | Limit all job submission (from any source) including jobnames, submitting userids, and execution userids |

Remediation:

Create generic resources for each of the high-level qualifiers in the list above to act as a backstop for each function or access according to the descriptions in the sections.

8.3.2 Ensure CANCEL JESJOBS profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a `CANCEL` high-level qualifier in the `JESJOBS` resource class control the use of the cancel SSI 2 (used by the `CANCEL TSO` command) and the cancel function of the job modify SSI 85. Canceling jobs can cause the job to terminate the current phase of processing and optionally purge the job from the system.

Rationale:

Failure to properly control access to canceling jobs could result in unauthorized personnel disrupting normal system operations or unauthorized users terminate required jobs

Audit:

Ensure the following items are in effect:

1. The `CANCEL.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `CANCEL.nodename.userid.jobname` resource in the `JESJOBS` class restricts `ALTER` access to the appropriate personnel (i.e., users allowed to cancel the specified jobname) and all access is logged.

NOTE: The user ID that owns a job is always allowed to `CANCEL` a job that they own regardless of any resource profiles




Remediation:

Ensure the following items are in effect:

1. The `CANCEL.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `CANCEL.nodename.userid.jobname` resource in the `JESJOBS` class restricts `ALTER` access to the appropriate personnel (i.e., users allowed to cancel the specified jobname) and all access is logged.
Examples of setting up proper protection are shown here:

```
RDEF JESJOBS CANCEL .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('Restrict CANCEL')  
PERMIT CANCEL.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(ALTER)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.3 Awareness of the ENCRYPT JESJOBS profiles (Manual)

Profile Applicability:

- Level 1

Description:

One way to encrypt data sets on SPOOL is to associate a KeyLabel with a JESJOBS resource with a high-level qualifier of `ENCRYPT`. This profile is not used to protect or audit use of KeyLabels, just to specify what KeyLabel is associated with a SYSOUT or instream data set. More information is available in the section on how to encrypt data set on SPOOL.

Rationale:

ENCRYPT resources are used to specify a KeyLabel to use to encrypt data and not used to restrict or audit access. It controls encryption of data set on SPOOL

Audit:

Remediation:

Define appropriate resources of the form:

```
ENCRYPT.nodename.userid.jobname.dsname
```

Specify the *KeyLabel* to use in the `KEYLABEL` field of the JES segment of the profile. Examples of setting up proper protection are shown here:

```
RDEF JESJOBS ENCRYPT.* UACC(READ) OWNER(ADMIN) JES(KEYLABEL(DEFAULTKEY)  
DATA('Encrypt everything'))
```

8.3.4 Ensure GROUPREG JESJOBS profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

JCL writers can define dependencies between job using a structure called a `JOBGROUP`. A `JOBGROUP` is a set of JCL that defines the dependencies between jobs and a set of JCL jobs streams that are part of the `JOBGROUP`. JESJOBS resources with a high-level qualifier of `GROUPREG` control what jobs can be added to a `JOBGROUP` when the owner of the `JOBGROUP` is not the same as the owner of the `JOB`. Failure to protect this resource may allow unauthorized users to add jobs to a `JOBGROUP` that they do not own.

Rationale:

It is expected that all jobs in a job group run under the same user authority. Though this is not required. This resource prevents an unauthorized user from adding their job to an existing `JOBGROUP`.

Audit:

Ensure the following items are in effect:

1. The `GROUPREG.nodename.grpname.userid` resource is defined to the JESJOBS resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `GROUPREG.nodename.grpname.userid` resource in the JESJOBS class restricts `READ` access to the appropriate personnel (i.e., users allowed to register jobs to the specified `grpname`) and all access is logged.

NOTE: The user ID that owns a `JOBGROUP` is always allowed to register a job that they own to a `JOBGROUP` without performing a check of the resource or generating an audit record.

Remediation:

Ensure the following items are in effect:




1. The `GROUPREG.nodename.grpname.userid` resource is defined to the JESJOBS resource class with a default access of NONE and all access is logged.
2. Access authorization to the `GROUPREG.nodename.grpname.userid` resource in the JESJOBS class restricts READ access to the appropriate personnel (i.e., users allowed to register jobs to the specified grpname) and all access is logged.

NOTE: The user ID that owns a JOBGROUP is always allowed to register a job that they own to a JOBGROUP without performing a check of the resource or generating an audit record.

Examples of setting up proper protection are shown here:

```
RDEF JESJOBS GROUPREG.* UACC(NONE) OWNER(ADMIN) DATA('JOBGROUP registration')  
PERMIT GROUPREG.nodename.grpname.userid CLASS(JESJOBS) ID() ACCESS(READ)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.5 Ensure *HOLD JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a `HOLD` high-level qualifier in the JESJOBS resource class control the use of the hold function of the job modify SSI 85. Holding a job delays processing until the job is released.

Rationale:

Failure to properly control access to holding jobs could result in unauthorized personnel disrupting normal system operations with unauthorized users holding required jobs.

Audit:

Ensure the following items are in effect:

1. The `HOLD.nodename.userid.jobname` resource is defined to the JESJOBS resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `HOLD.nodename.userid.jobname` resource in the JESJOBS class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to hold the specified jobname) and all access is logged.




Remediation:

Ensure the following items are in effect:

1. The `HOLD.nodename.userid.jobname` resource is defined to the JESJOBS resource class with a default access of NONE and all access is logged.
2. Access authorization to the `HOLD.nodename.userid.jobname` resource in the JESJOBS class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to hold the specified jobname) and all access is logged.
Examples of setting up proper protection are shown here:

```
RDEF JESJOBS HOLD .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('Restrict  
HOLD')  
PERMIT HOLD.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(UPDATE)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.6 Ensure *JOBCLASS JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a *JOBCLASS* high-level qualifier in the *JESJOBS* resource class control the use of the job classes. Attributes of a job class such as bypass label processing (BLP) need to be restricted to appropriate users. Additionally, job classes can be associated with batch initiators that are reserved for appropriate applications.

Rationale:

Failure to properly control job class usage could result in unauthorized personnel disrupting normal system operations and using a job class reserved for a specific purpose.

Audit:

If job class protection is required, ensure the following items are in effect:




1. Enable protection by defining one or both of the following non-generic profiles in the *FACILITY* class:
JES.JOBCLASS.SUBMITTER - verify job submitter access to the job class
JES.JOBCLASS.OWNER - verify job owner access to the job class
2. The *JOBCLASS.** resource is defined to the *JESJOBS* resource class with a default access of *READ* and all access is logged.
3. Define *JOBCLASS.nodename.jobclass.jobname* resource to the *JESJOBS* resource class with a default access of *NONE* and all access is logged for each job class that needs to be controlled.
4. Access authorization to the *JOBCLASS.nodename.jobclass.jobname* resource in the *JESJOBS* class restricts *READ* access to the appropriate users and all access is logged.

Remediation:

If job class protection is required, ensure the following items are in effect:

- 1. Enable protection by defining one or both of the following non-generic profiles in the FACILITY class:
JES.JOBCLASS.SUBMITTER - verify job submitter access to the job class
JES.JOBCLASS.OWNER - verify job owner access to the job class
- 2. The JOBCLASS.* resource is defined to the JESJOBS resource class with a default access of READ and all access is logged.
- 3. Define JOBCLASS.nodename.jobclass.jobname resource to the JESJOBS resource class with a default access of NONE and all access is logged for each job class that needs to be controlled.
- 4. Access authorization to the JOBCLASS.nodename.jobclass.jobname resource in the JESJOBS class restricts READ access to the appropriate users and all access is logged.
Alternatively, if jobname usage is being controlled by SUBMIT resource profiles, you could define JOBCLASS.nodename.jobclass.* with a UACC of NONE and then a resource with allowed job names JOBCLASS.nodename.jobclass.jobname with a UACC of READ,

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.7 Ensure JOBNFY JESJOBS profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a MODIFY high-level qualifier in the JESJOBS resource class control the use of the HTTP post notification of job status. Users of the JOBS REST API (and the internal reader) can specify an address where a HTTP POST notification is sent when certain job transitions occur (such as the job completes).

Rationale:

Use of HTTP POST function may need to be restricted to limit use of HTTP POST function

Audit:

Ensure the following items are in effect:

1. The JOBNFY.nodename.jobclass.jobname resource is defined to the JESJOBS resource class with a default access of NONE and all access is logged.
2. Access authorization to the JOBNFY.nodename.jobclass.jobname resource in the JESJOBS class restricts READ access to the appropriate personnel and all access is logged.

Remediation:




Ensure the following items are in effect:

1. The `JOBNFY.nodename.jobclass.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `JOBNFY.nodename.jobclass.jobname` resource in the `JESJOBS` class restricts `READ` access to the appropriate personnel and all access is logged.

Examples of setting up proper protection are shown here:

```
RDEF JESJOBS JOBNFY .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('Restrict HTTP POST')
PERMIT JOBNFY.nodename.jobclass.jobname CLASS(JESJOBS) ID() ACCESS(READ)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.8 Ensure *MODIFY JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a MODIFY high-level qualifier in the JESJOBS resource class control the use of the modify job function of the job modify SSI 85. Modifying a job can change the attributes of a job such as the job class, service class, system affinity, and priority.

Rationale:

Failure to properly control access to modifying jobs could result in unauthorized personnel disrupting normal system operations by modifying required jobs.

Audit:

Ensure the following items are in effect:

1. The `MODIFY.nodename.userid.jobname` resource is defined to the JESJOBS resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `MODIFY.nodename.userid.jobname` resource in the JESJOBS class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to modify the specified jobname) and all access is logged.




Remediation:

Ensure the following items are in effect:

1. The `MODIFY.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `MODIFY.nodename.userid.jobname` resource in the `JESJOBS` class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to modify the specified jobname) and all access is logged.
Examples of setting up proper protection are shown here:

```
RDEF JESJOBS MODIFY .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('Restrict MODIFY')  
PERMIT MODIFY.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(UPDATE)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.9 Ensure *PURGE JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a PURGE high-level qualifier in the JESJOBS resource class control the use of the purge function of the job modify SSI 85. Purging a job removes the job from the system.

Rationale:

Failure to properly control access to purging jobs could result in unauthorized personnel disrupting normal system operations by purging required jobs.

Audit:

Ensure the following items are in effect:

1. The `PURGE.nodename.userid.jobname` resource is defined to the JESJOBS resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `PURGE.nodename.userid.jobname` resource in the JESJOBS class restricts `ALTER` access to the appropriate personnel (i.e., users allowed to purge the specified jobname) and all access is logged.




Remediation:

Ensure the following items are in effect:

1. The `PURGE.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `PURGE.nodename.userid.jobname` resource in the `JESJOBS` class restricts `ALTER` access to the appropriate personnel (i.e., users allowed to purge the specified jobname) and all access is logged.
Examples of setting up proper protection are shown here:

```
RDEF JESJOBS PURGE .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('Restrict  
PURGE')  
PERMIT PURGE.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(ALTER)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.10 Ensure *RELEASE JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a RELEASE high-level qualifier in the JESJOBS resource class control the use of the release function of the job modify SSI 85. Releasing a job could allow a job to begin processing prematurely.

Rationale:

Failure to properly control access to releasing jobs could result in unauthorized personnel disrupting normal system operations and unauthorized users releasing required jobs.

Audit:

Ensure the following items are in effect:

1. The `RELEASE.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `RELEASE.nodename.userid.jobname` resource in the `JESJOBS` class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to release the specified jobname) and all access is logged.




Remediation:

Ensure the following items are in effect:

1. The `RELEASE.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `RELEASE.nodename.userid.jobname` resource in the `JESJOBS` class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to release the specified jobname) and all access is logged.
Examples of setting up proper protection are shown here:

```
RDEF JESJOBS RELEASE .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('Restrict RELEASE ')
PERMIT RELEASE.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(UPDATE)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.11 Ensure *REROUTE JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a `REROUTE` high-level qualifier in the `JESJOBS` resource class control the use of the `reroute` function of the job modify SSI 85. Rerouting a job sends a job (with any instream data) to another NJE node for execution (or could cause an NJE bound job to execute locally).

Rationale:

Failure to properly control access to rerouting jobs could result in unauthorized personnel disrupting normal system operations and potentially sending a job with sensitive instream data to a different NJE node. Unauthorized users rerouting a job could expose the contents of the job (and any instream data) to an unintended NJE node

Audit:

Ensure the following items are in effect:

1. The `REROUTE.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `REROUTE.nodename.userid.jobname` resource in the `JESJOBS` class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to reroute the specified jobname) and all access is logged.




Remediation:

Ensure the following items are in effect:

1. The `REROUTE.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `REROUTE.nodename.userid.jobname` resource in the `JESJOBS` class restricts `UPDATE` access to the appropriate personnel (i.e., users allowed to reroute the specified jobname) and all access is logged.
Examples of setting up proper protection are shown here:

```
RDEF JESJOBS REROUTE .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('Restrict REROUTE ')
PERMIT REROUTE.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(UPDATE)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.12 Ensure SPIN JESJOBS profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a `SPIN` high-level qualifier in the `JESJOBS` resource class control the use of the spin function of the job modify SSI 85. Spinning a job caused all SPIN output of a job to be made available for immediate processing (rather than waiting for the job to end). SPIN output could include logs associated with the running job. Processing could include purging of the data sets that were spun.

Rationale:

Failure to properly control access to spinning jobs could result in unauthorized personnel making data available for processing (or purging) before the job completes.

Audit:

Ensure the following items are in effect:

1. The `SPIN.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `SPIN.nodename.userid.jobname` resource in the `JESJOBS` class restricts `CONTROL` access to the appropriate personnel (i.e., users allowed to SPIN the output for the specified jobname) and all access is logged.

Remediation:




Ensure the following items are in effect:

- 1. The SPIN.nodename.userid.jobname resource is defined to the JESJOBS resource class with a default access of NONE and all access is logged.
- 2. Access authorization to the SPIN.nodename.userid.jobname resource in the JESJOBS class restricts CONTROL access to the appropriate personnel (i.e., users allowed to SPIN the output for the specified jobname) and all access is logged.

Examples of setting up protection are shown here:

```
RDEF JESJOBS SPIN .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('Restrict
SPIN ')
PERMIT SPIN.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(CONTROL)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.13 *Ensure SPOOLIO JESJOBS profiles are protected (Manual)*

Profile Applicability:

- Level 1

Description:

Resources with a `SPOOLIO` high-level qualifier in the `JESJOBS` resource class control the use of the SPOOL I/O function of the job information SSI 71. The SPOOL I/O function is intended for application to access data on the JES2 spool for debugging purposes.

Rationale:

Failure to properly control access to spool I/O could result in unauthorized personnel accessing sensitive or confidential customer data. Most access to SPOOL control blocks is managed by the JESSPOOL resource class. However, that use requires that the data can be associated with a specific existing job. In the case where the data being accessed is not associated with a job or the job no longer exists, this JESJOBS resource class check is used. Ensure that access authorization for SPOOLIO resources is restricted to Systems personnel responsible for diagnosing JES2 and z/OS problems.

Audit:

Ensure the following items are in effect:

1. The `SPOOLIO.nodename.jobname.jobid.cbname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `SPOOLIO.nodename.jobname.jobid.cbname` resource in the `JESJOBS` class restricts `READ` access to the appropriate personnel (i.e., Systems personnel responsible for diagnosing JES2 and z/OS problems) and all access is logged.

Remediation:




Ensure the following items are in effect:

1. The `SPOOLIO.nodename.jobname.jobid.cbname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `SPOOLIO.nodename.jobname.jobid.cbname` resource in the `JESJOBS` class restricts `READ` access to the appropriate personnel (i.e., Systems personnel responsible for diagnosing JES2 and z/OS problems) and all access is logged.

Examples of setting up protection are shown here:

```
RDEF JESJOBS SPOOLIO .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))
DATA('Restrict SPOOL read ')
PERMIT SPOOLIO.nodename.jobname.jobid.cbname CLASS(JESJOBS) ID() ACCESS(READ)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|--|--|--|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.14 Ensure START JESJOBS profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a `START` high-level qualifier in the `JESJOBS` resource class control the use of the start function of the job modify SSI 85. Starting a job causes a job to begin processing immediately (starting an initiator if required). This could cause a job to begin processing prematurely.

Rationale:

Failure to properly control access to starting jobs could result in unauthorized personnel starting jobs prematurely or starting more jobs than the system has capacity to process.

Audit:

Ensure the following items are in effect:

1. The `START.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `START.nodename.userid.jobname` resource in the `JESJOBS` class restricts `CONTROL` access to the appropriate personnel (i.e., users allowed to start the specified jobname) and all access is logged.

Remediation:




Ensure the following items are in effect:

1. The `START.nodename.userid.jobname` resource is defined to the `JESJOBS` resource class with a default access of `NONE` and all access is logged.
2. Access authorization to the `START.nodename.userid.jobname` resource in the `JESJOBS` class restricts `CONTROL` access to the appropriate personnel (i.e., users allowed to start the specified jobname) and all access is logged.

Examples of setting up protection are shown here:

```
RDEF JESJOBS START .* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('Restrict  
START ')  
PERMIT START.nodename.userid.jobname CLASS(JESJOBS) ID() ACCESS(CONTROL)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.3.15 Ensure *SUBMIT JESJOBS* profiles are protected (Manual)

Profile Applicability:

- Level 1

Description:

Resources with a `SUBMIT` high-level qualifier in the `JESJOBS` resource class control the submitting of batch jobs from all sources. By using these resources, you can control the combination of job names, owning user IDs, and submitting user IDs that can be used.

Rationale:

Typically, resources of this type are used when the use of job names must be restricted to certain owning user IDs or submitting user IDs. This would be the case if job names are used to control other concepts such as encryption. They can also be used to limit what jobs a user can submit or what user IDs can be used with batch jobs.

NOTE: Creating a `SUBMIT.*` profile with a UACC of `NONE` blocks all batch job submission. Generally, the `SUBMIT.*` profile is created with a UACC of `READ` and then more specific profiles are created with a UACC of `NONE` to restrict unauthorized job submissions.

Audit:

Ensure the following items are in effect:

1. The `SUBMIT.nodename.jobname.userid` resource is defined to the `JESJOBS` resource class with a default access of `READ` and all access is logged.
2. Access authorization to the `SUBMIT.nodename.jobname.userid` resource in the `JESJOBS` class restricts `NONE` access to for the combinations that require restricted usage with all access is logged.

NOTE: Creating a `SUBMIT.*` profile with a UACC of `NONE` blocks all batch job submission.

Remediation:

Ensure the following items are in effect:

1. The `SUBMIT.nodename.jobname.userid` resource is defined to the `JESJOBS` resource class with a default access of `READ` and all access is logged.
2. Access authorization to the `SUBMIT.nodename.jobname.userid` resource in the `JESJOBS` class restricts `NONE` access to for the combinations that require restricted usage with all access is logged.

Examples of setting up proper protection are shown here:

```
RDEF JESJOBS START .* UACC(READ) OWNER(ADMIN) AUDIT(ALL(READ)) DATA('Allow  
general SUBMIT ')
```




Control users that can submit jobs that start with `PROD*`

```
RDEF JESJOBS START *.*.PROD*.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('Contol PROD* jobnames ')  
PERMIT START *.*.PROD*.* CLASS(JESJOBS) ID() ACCESS(READ)
```

Jobs that start with `PROD*` can only be run by the `PRODUSER` user ID

```
RDEF JESJOBS START *.*.PROD*.* UACC(NONE) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('Contol PROD* jobnames ')  
RDEF JESJOBS START *.*.PROD*.PRODUSER UACC(READ) OWNER(ADMIN) AUDIT(ALL(READ))  
DATA('PROD* jobnames must have PRODUSER id')
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.4 Enable Encryption of Data Set on SPOOL

This section describes the Enable Encryption of Data Set on SPOOL recommendations.

8.4.1 Ensure that data sets on SPOOL are encrypted as required (Manual)

Profile Applicability:

- Level 1

Description:

Job data sets (instream and SYSOUT data sets) can be encrypted using profiles in the `JESJOBS` class with a high-level qualifier of `ENCRYPT`. The *KeyLabel* for encryption is set in the JES segment of the profile.

Rationale:

Encrypting data sets on SPOOL provides an extra level of security for the data. Access to the data requires both access via the JESSPOOL class and access to the key label used to encrypt the data. It also limits the exposure to inadvertent access to SPOOL buffers.

Audit:

There are two ways to request encryption of data on spool:

- Specify key labels in the JESJOBS resource class profiles. This is done using the `KEYLABEL` keyword in the JES segment of the `JESJOBS` resource class profile `ENCRYPT.nodename.userid.jobname.dsname`
- Specify the `DSKEYLBL=` keyword on the DD statement for instream data (DD * or DD DATA) or SYSOUT (DD SYSOUT=). In order to specify `DSKEYLBL` the user must have `READ` access to one of the two `FACILITY` class profiles.
`JES.ENCRYPT.OWNER` for SYSOUT and instream data in PROCs and INCLUDEs.
`JES.ENCRYPT.SUBMITTER` for all other instream data sets (processed during input phase).

Remediation:

There are two ways to request encryption of data on spool:

- Specify key labels in the JESJOBS resource class profiles. This is done using the `KEYLABEL` keyword in the JES segment of the JESJOBS resource class profile `ENCRYPT.nodename.userid.jobname.dsname`
- Specify the `DSKEYLBL=` keyword on the DD statement for instream data (DD * or DD DATA) or SYSOUT (DD SYSOUT=). In order to specify DSKEYLBL the user must have READ access to one of the two FACILITY class profiles.

`JES.ENCRYPT.OWNER` for SYSOUT and instream data in PROCs and INCLUDEs.

`JES.ENCRYPT.SUBMITTER` for all other instream data sets (processed during input phase).

Examples of setting up proper protection are shown here:

```
RDEF JESJOBS ENCRYPT.* UACC(READ) OWNER(ADMIN) JES(KEYLABEL(DEFAULTKEY)
DATA('Encrypt everything'))
RDEF JESJOBS ENCRYPT.nodename.PRODUSER.* UACC(READ) OWNER(ADMIN)
JES(KEYLABEL(PRODKEY)) DATA('Encrypt production stuff')
RDEF FACILITY JES.ENCRYPT.OWNER UACC(READ) OWNER(ADMIN) DATA('Allow
DSKEYLBL=')
```

8.4.2 Require user identification (Manual)

Profile Applicability:

- Level 1

Description:

SETROPTS BATCHALLRACF specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch JOBS. The system-wide option controls the default settings for determining how RACF will function when handling requests for access to the operating system environment, RACF, and customer data.

Rationale:

For proper logging and verification of batch job, all jobs must have a validated user ID. Failure to set this option will allow jobs to run on the system without being identified and verified by RACF.

Audit:

Issue the following command from TSO

```
SETROPTS LIST
```

Ensure JES-BATCHALLRACF is active.

Remediation:

Issue the following command from TSO

```
SETROPTS LIST
```

Ensure JES-BATCHALLRACF is active.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223692 Rule ID: SV-223692r604139_rule STIG ID: RACF-ES-000440 Severity: CAT II

8.4.3 Ensure that the JES(BATCHALLRACF) SETROPTS value is set to JES(BATCHALLRACF) (Manual)

Profile Applicability:

- Level 1

Description:

SETROPTS BATCHALLRACF specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch JOBS. The system-wide option controls the default settings for determining how RACF will function when handling requests for access to the operating system environment, RACF, and customer data.

Rationale:

For proper logging and verification of batch job, all jobs must have a validated user ID. Failure to set this option will allow jobs to run on the system without being identified and verified by RACF.

Audit:

Issue the following command from TSO.

```
SETROPTS LIST
```

Ensure JES-BATCHALLRACF is active.

Remediation:

Issue the following command from TSO.

```
SETROPTS LIST
```

Ensure JES-BATCHALLRACF is active.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223692 Rule ID: SV-223692r604139_rule STIG ID: RACF-ES-000440 Severity: CAT II

8.4.4 Ensure that the JES(XBMALLRACF) SETROPTS value is set to JES(XBMALLRACF) (Manual)

Profile Applicability:

- Level 1

Description:

XBM (execution batch monitor) is a function that allows jobs to be submitted that only provide instream data to a pre-defined JCL PROC. The classic use of this is to perform student compiles in an educational environment. Even though the JCL PROC is pre-defined, proper auditing of what the JCL is accessing requires that a RACF identity exists for all jobs. XBM is configured by specifying a value for XBM= on a JOBCLASS statement. Use the command \$DJOBCLASS(*),XBM!=,XBM to determine if XBM is in use.

XBMALLRACF ensures that (assuming you have JES configured to support XBM jobs) any XBM job submitted by a user must have a RACF identity or the job will fail. This is used only in JES2.

Rationale:

Failure to set XBMALLRACF will allow XBM jobs run on a system without a proper RACF identity.

Audit:

If JES(XBMALLRACF) is enabled the message "JES-XBMALLRACF OPTION IS ACTIVE" will be displayed.

Remediation:

Ensure that JES(XBMALLRACF) SETROPTS value is set to JES (XBMALLRACF) . This specifies that JES is set to test for a user ID and password on the job statement or for propagated RACF identification information for all jobs run under the execution batch monitor.

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the control option as specified in the example below: RACF Command SETR LIST will show the status of RACF Controls including a status of

JES-XBMALLRACF.

XBMALLRACF is activated with the command:

```
SETR XBMALLRACF
```


References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223693 Rule ID: SV-223693r604139_rule STIG ID: RACF-ES-000460 Severity: CAT II

8.5 Control Access to Data Sets Used by JES2

This section describes the Enable Encryption of Control Access to Data Sets Used by JES2 recommendations.

8.5.1 Ensure that access (read, update and allocate) to the data sets used by JES2 is controlled (Manual)

Profile Applicability:

- Level 1

Description:

The JES2 System data sets are a common repository for all jobs submitted to the system and the associated printout and configuration of the JES2 environment. Initialization data sets can contain NJE and RJE signon passwords and need to be protected unintended access. These include:

- JES2 initialization parameters
- JES2 checkpoint data sets
- JES2 SPOOL data sets

Rationale:

Allowing READ access to the SPOOL data set would allow an unauthorized user to access any data that resides on spool compromising the confidentiality of customer data.

Audit:

Ensure only JES2 needs access to the data sets that it uses. Access to checkpoint and spool data sets should be set to `NONE`.

Access to the initialization parameter data sets should be restricted to appropriate personnel responsible for maintaining JES2. In particular any data set that may contain Line or node passwords.

Remediation:

Confirm that trace files are covered by a RACF DATASET profile with the following attributes:

- `UACC(NONE)`
- No `ID(*)` on the access list
- Not in `WARNING` mode
- Access is restricted to system programmers and started tasks that perform GTF processing
- All accesses are being logged

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223690 Rule ID: SV-223690r604139_rule STIG ID: RACF-ES-000420 Severity: CAT II

8.5.2 Ensure that access to any PROCLIB data sets used by JES2 is protected from unintended updates (Manual)

Profile Applicability:

- Level 1

Description:

PROCLIB data sets contain the steps (programs) that a job (or started task) will run. They can also contain instream data that control those programs. Altering the steps in a PROC could allow an unintended program to get control under the user authority of the job (or started task) using the PROC.

Data sets in a PROCLIB concatenation (specified in the JES2 PROC or using PROCLIB statements) are access using the authority of JES2. Jobs do not require any access to these data sets to use a JCL PROC contained within them.

Data sets accessed via a JCLLIB JCL statement, however, are accessed using the owning user ID associated with the job and require READ access to data sets in JCLLIB.

Rationale:

Unauthorized users altering PROCs in a PROCLIB data set can cause unintended program to run under the authority of the user ID that owns the job using the PROC.

Audit:

Refer to the following for the PROCLIB data sets that contain the STCs and TSO logons from the following sources:

- MSTJCLxx member used during an IPL. The PROCLIB data sets are obtained from the IEFPSI and IEFJOBS DD statements.
- PROCxx DD statements in the JES2 PROC. Where 'xx' is the PROCLIB entries for the STC and TSU JOBCCLASS configuration definitions.
- PROCLIB(nnnnnnnn) JES2 initialization statements or commands. Use the following command to determine the full list of JES2 PROCLIBs.

```
$D PROCLIB (*)
```

Verify that the accesses to the above PROCLIB data sets are properly restricted. Check that the ESM data set access authorizations restrict WRITE and/or greater access to systems programming personnel.

Remediation:

Use the `$D PROCLIB(*)` command to get a complete list of data sets used for PROBLIB:




```
PROCLIB(PROC00)    STATIC LIBRARY,
                   DD(1)=(DSNAME=SYS1.PROCLIB,      <== Data set name
                   VOLSER=J2SHR2,UNIT=SYSALLDA) ,
                   DD(2)=(DSNAME=SYS1.PROCLIB,
                   VOLSER=J2SHR2,UNIT=SYSALLDA) ,
                   DD(3)=(DSNAME=SYS1.PROCLIB,
                   VOLSER=J2SHR2,UNIT=SYSALLDA)
$HASP319 PROCLIB(PROC01)
PROCLIB(PROC01)    STATIC LIBRARY,
                   DD(1)=(DSNAME=SYS1.PROCLIB,
                   VOLSER=J2SHR2,UNIT=SYSALLDA)
$HASP319 PROCLIB(PROC02)
PROCLIB(PROC02)    DD(1)=(DSNAME=SYS1.PROCLIB,
                   VOLSER=J2SHR2) ,
                   DD(2)=(DSNAME=SYS1.PROCLIB.POK,
                   VOLSER=ZDR31) ,
                   DD(3)=(DSNAME=SYS1.PROCLIB.INSTALL,
                   VOLSER=ZDR31)
```

Use the ESM data set authorization to restrict write and/or greater access to appropriate system programming personnel.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223687 Rule ID: SV-223687r604139_rule STIG ID: RACF-ES-000390 Severity: CAT I

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.5.3 Ensure that RACF is called for data sets opened by JES2 (Manual)

Profile Applicability:

- Level 1

Description:

The program property table provides an option to bypass password checking for data sets (NOPASS). This causes OPEN processing to bypass the call to RACF data set access authorization for the specified address space. JES2 is defined with the attribute PASS which requires that RACF be called for all data set access.

Rationale:

Specifying PASS for the PPT entry for JES2 (HASJES20) is required to ensure that access to JCLLIB data sets is properly authorized. Specifying NOPASS for HASJES20 (the JES2 PPT entry) would allow a JCLLIB JCL statement to access any data set. If the data set were a PDS with a record format of F and a record length of 80, during JCL conversion the data set would be read and its contents displayed as error message in the JCL listing. This could compromise the confidentiality of customer data.

Audit:

Use the command:

```
D PPT
```

to get a list of the current PPT attributes on the system and ensure that the entry for JES2 does not specify NOPASS. The “NP” column should indicate “.”.

Sample output:

| PgmName | NC | NS | PR | ST | ND | BP | Key | 2P | 1P | NP | NH | CP | DA | PA |
|----------|----|----|----|----|----|----|-----|----|----|----|----|----|----|----|
| HASJES20 | Y | Y | . | Y | Y | . | 1 | . | . | . | Y | . | . | . |

Remediation:

Update the SHEDxx PARMLIB member listed in the output of the D PPT command to remove the NOPASS specification for HASJES20

8.6 Device Management

This section describes the Enable Encryption of Device Management recommendations.

8.6.1 Ensure that JES2 output devices are controlled (Manual)

Profile Applicability:

- Level 1

Description:

JES2 output devices provide a variety of channels to which output can be processed. Failure to properly control these output devices could result in unauthorized personnel accessing output.

Rationale:

Profiles in the WRITER resource class can control what devices and destination a job can access. Most WRITER checks are made when the SYSOUT is selected to be printed. If the owner does not have access to the device (as defined by the WRITER resource class profile) then the output is not processed (and remains on SPOOL).

NJE destination checks (JES2.NJE.nodename) are performed at the time the SYSOUT is being allocated. If the owning user ID does not have access to the NJE node, the SYSOUT allocation is failed.

Failure to control output devices could result in SYSOUT being printed on an inappropriate device.

Audit:

Refer the JES2PARM member of SYS1.PARMLIB.

Review the following resources in the RACF WRITER resource class:

```
JES2.** (backstop profile)
JES2.LOCAL.OFFn.* (spool offload transmitter)
JES2.LOCAL.OFFn.ST (spool offload SYSOUT transmitter)
JES2.LOCAL.OFFn.JT (spool offload job transmitter)
JES2.LOCAL.PRTn (local printer)
JES2.LOCAL.PUNn (local punch)
JES2.NJE.nodename (NJE node)
JES2.RJE.Rnnnn.PRm (remote printer)
JES2.RJE.Rnnnn.PUm (remote punch)
```

JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

- OFFn, where n is the number of the offload transmitter. Determine the numbers by searching for OFF(in the JES2 parameters.
- PRTn, where n is the number of the local printer. Determine the numbers by searching for PRT(in the JES2 parameters.
- PUNn, where n is the number of the local card punch. Determine the numbers by searching for PUN(in the JES2 parameters
- Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report.
- Rnnnn.PRm, where nnnn is the number of the remote workstation and m is the number of the printer. Determine the numbers by searching for .PR in the JES2 parameters.
- Rnnnn.PUm, where nnnn is the number of the remote workstation and m is the number of the punch. Determine the numbers by searching for .PU in the JES2 parameters.

Check that the WRITER resource class is active.

Check that the other resources detailed above are protected by generic and/or fully qualified profiles defined to the WRITER resource class with UACC(NONE) .

Remediation:

Review the following resources in the WRITER resource class:

```
JES2.** (backstop profile)
JES2.LOCAL.OFFn.* (spool offload transmitter)
JES2.LOCAL.OFFn.ST (spool offload SYSOUT transmitter)
JES2.LOCAL.OFFn.JT (spool offload job transmitter)
JES2.LOCAL.PRTn (local printer)
JES2.LOCAL.PUNn (local punch)
JES2.NJE.nodename (NJE node)
JES2.RJE.Rnnnn.PRm (remote printer)
JES2.RJE.Rnnnn.PUm (remote punch)
```

JES2 is typically the name of the JES2 subsystem. Refer to the SUBSYS report and locate the entry with the description of PRIMARY JOB ENTRY SUBSYSTEM. The SUBSYSTEM NAME of this entry is the name of the JES2 subsystem.

- OFFn, where n is the number of the offload transmitter. Determine the numbers by searching for OFF(in the JES2 parameters.
- PRTn, where n is the number of the local printer. Determine the numbers by searching for PRT(in the JES2 parameters.
- PUNn, where n is the number of the local card punch. Determine the numbers by searching for PUN(in the JES2 parameters.
- Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions by searching for NODE(in the report.
- Rnnnn.PRm, where nnnn is the number of the remote workstation and m is the number of the printer. Determine the numbers by searching for .PR in the JES2 parameters.
- Rnnnn.PUm, where nnnn is the number of the remote workstation and m is the number of the punch. Determine the numbers by searching for .PU in the JES2 parameters.

Define the WRITER resource class to the ACTIVE CLASSES in RACF SETROPTS.

Configure the profile JES2.** to have no access in the WRITER resource class.

Configure the resources detailed above to be protected by generic and/or fully qualified profiles defined to the WRITER resource class.

Examples:

```




setr classact(writer)
setr gencmd(writer) generic(writer)
setr raclist(writer)
RDEF WRITER JES2.** owner(admin) AUDIT(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.** owner(admin) AUDIT(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.JT owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.OFF*.ST owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PRT* owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.LOCAL.PUN* owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.NJE.** owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
RDEF WRITER JES2.RJE.** owner(admin) audit(ALL) UACC(NONE) -
data('Reference SRR PDI ZJES0031')
pe JES2.** cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.** cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.OFF*.JT cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.OFF*.ST cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.PRT* cl(writer) id(<syspsmpl>)
pe JES2.LOCAL.PUN* cl(writer) id(<syspsmpl>)
pe JES2.NJE.** cl(writer) id(<syspsmpl>)
pe JES2.RJE.** cl(writer) id(<syspsmpl>)
setr racl(writer) Ref

```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223748 Rule ID: SV-223748r604139_rule STIG ID: RACF-JS-000040 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.6.2 Ensure that bypass label processing (BLP=) is not set on any JOBCLASS (Manual)

Profile Applicability:

- Level 1

Description:

BLP=YES on a JOBCLASS statement allows certain security checks to be skipped when accessing certain tape data set. There are other ways to manage this setting than the JOBCLASS statement. See <https://www.ibm.com/docs/en/zos/2.5.0?topic=tape-racf-authorization-bypass-label-processing-blp> for details on how to properly set this.

Rationale:

Using BLP=YES on a JOBCLASS statement could expose data on tapes. It is possible to limit what user IDs could use a JOBCLASS with BLP=YES, but a better way would be use RACF to manage the processing.

Audit:

Use the JES2 command to display the current setting of the BLP parameter.

```
$D JOBCLASS (*),BLP
e.g.
$D JOBCLASS (A),BLP
$HASP837 JOBCLASS (A)          BLP=NO
```

Remediation:

Use the command to alter the current BLP processing for any job class that specified BLP=YES.

```
$T JOBCLASS (x) , BLP=NO
e.g.
$T JOBCLASS (A) , BLP=NO
```

Also examine the JES2 initialization parameters to determine if the BLP=YES specification is specified.

Note that the JOBCLASS specifications in the initialization parameters only apply when a JES2 system is COLD started (the saved settings are used on all warm starts). Examining the setting in the initialization parameters is not sufficient to determine what the system is actually using.

To determine the initialization data sets being used by this JES2 instance, use the command:

```
$D INITINFO
      $HASP825 INITINFO
$HASP825 INITINFO --- Command used to start JES2
$HASP825          S JES2,N=ZOS203,M=SPOOLZ23,PARM=(COLD,NOREQ)
$HASP825          --- HASPPARM data sets read
$HASP825          DSN=SYS1.PARMLIB(SPOOLZ23),VOLSER=J2SHR2,
$HASP825          CARDS=462,
$HASP825          DSN=SYS1.PARMLIB(DYEXIT21),CARDS=124,
$HASP825          DSN=SYS1.PARMLIB(NULL),VOLSER=J2SHR2,CARDS=1
```

8.6.3 Ensure that use of JES2 input sources are controlled (Manual)

Profile Applicability:

- Level 1

Description:

JES2 input sources provide a variety of channels for job submission. Failure to properly control the use of these input sources could result in unauthorized submission of work into the operating system.

Rationale:

This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Review the following resources in the JESINPUT resource class:

| | |
|------------|-------------------------------------|
| `INTRDR` | (internal reader for batch jobs) |
| `nodename` | (NJE node) |
| `OFFn.*` | (spool offload receiver) |
| `Rnnnn` | (RJE workstation) |
| `RDRnn` | (local card reader) |
| `STCINRDR` | (internal reader for started tasks) |
| `TSUINRDR` | (internal reader for TSO logons) |

NOTE: If any of the following are not defined within the JES2 parameters, the resource in the JESINPUT resource class does not have to be defined.

NOTE 1: Nodename is the NAME parameter in the NODE statement.

NOTE 2: OFFn, where n is the number of the offload receiver.

NOTE 3: Rnnnn, where nnnn is the number of the remote workstation.

NOTE 4: RDRnn, where nn is the number of the reader.

Ensure the following items are in effect:

1. The JESINPUT resource class is active.
2. The resources mentioned above are protected by generic and/or fully qualified profiles defined to the JESINPUT resource class.
3. UACC(NONE) is specified for all resources.
NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs for all users. No guidance on which input sources are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, offload, and STC input sources.

Remediation:



Ensure the following items are in effect:

1. The JESINPUT resource class is active.
2. The resources below are protected by generic and/or fully qualified profiles defined to the JESINPUT resource class.
 - INTRDR (internal reader for batch jobs)
 - nodename (NJE node)
 - OFFn.* (spool offload receiver)
 - Rnnnn (RJE workstation)
 - RDRnn (local card reader)
 - STCINRDR (internal reader for started tasks)
 - TSUINRDR (internal reader for TSO logons)
3. UACC(NONE) is specified for all resources.
NOTE: UACC(READ) is allowed for input sources that are permitted to submit jobs for all users. Currently, there is no guidance on which input sources are appropriate for UACC(READ). However, common sense should prevail during the analysis. For example, UACC(READ) would typically be inappropriate for RJE, NJE, offload, and STC input sources.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223747 Rule ID: SV-223747r604139_rule STIG ID: RACF-JS-000030 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.7 JES2 Networking

This section describes the JES2 Networking recommendations.

8.7.1 Ensure that RJE workstations and NJE nodes are controlled (Manual)

Profile Applicability:

- Level 1

Description:

JES2 RJE workstations and NJE nodes provide a method of sending and receiving data (e.g., jobs, job output, and commands) from remote locations. Failure to properly identify and control these remote facilities could result in unauthorized sources transmitting data to and from the operating system. This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Rationale:

Audit:

Refer to

| |
|--------------------------------------|
| <code>SYS1.PARMLIB (JES2PARM)</code> |
|--------------------------------------|

For each node entry check that all JES2 defined NJE nodes and RJE workstations have a profile defined in the `FACILITY` resource class.

NOTE: NJE.* and RJE.* profiles will force user ID and password protection of all NJE and RJE connections respectively. This method is acceptable in lieu of using discrete profiles.




Remediation:

Configure associated PROFILES TO exist for all RJE/NJE sources and review the authorizations for these remote facilities.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223745 Rule ID: SV-223745r604139_rule STIG ID: RACF-JS-000010 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

8.7.2 Ensure that RJE workstations and NJE nodes are controlled (Manual)

Profile Applicability:

- Level 1

Description:

JES2 RJE workstations and NJE nodes provide a method of sending and receiving data (e.g., jobs, job output, and commands) from remote locations. Failure to properly identify and control these remote facilities could result in unauthorized sources transmitting data to and from the operating system.

Rationale:

This exposure may threaten the integrity and availability of the operating system environment and compromise the confidentiality of customer data.

Audit:

Review the JES2 parameters for RJE workstation definitions by searching for RMT(in the report.

Ensure the RJE workstation user IDs are defined as follows:

1. A user ID of RMTnnnn is defined to RACF for each RJE workstation, where nnnn is the number on the RMT statement.
2. No user ID segments (e.g., TSO, CICS, etc.) are defined.
3. Restricted from accessing all data sets and resources with exception of the corresponding JESINPUT class profile for that remote.

Remediation:

RJE user IDs

Note that this guidance addresses RJE Workstations that are "Dedicated". If an RJE workstation is dedicated, the assumption is that the RJE to host connection is hard-wired between the RJE and host. In this case the RMT definition statement will contain the keyword `LINE=` which specifies that this RJE is only connected via that one `LINE` statement.

a) Review the JES2 parameters for RJE workstation definitions

b) Ensure the RJE workstation user IDs are defined as follows:

- A user ID of `RMTnnnn` is defined to RACF for each RJE workstation, where `nnnn` is the number on the RMT statement.
- No user ID segments (e.g., TSO, CICS, etc.) are defined.
- Restricted from accessing all data sets and resources with exception of the corresponding JESINPUT-class profile for that remote.

Review Chapter 17 of RACF Security Admin Guide. The following is an example that show proper implementation:

```
AG RMTGRP OWNER(ADMIN) SUPGROUP(ADMIN)
AU RMT777 NAME('RMT RJE 777') DFLTGRP(RMTGRP) OWNER(RMTGRP) DATA('COMPLY WITH
ZJES0011') NOPASS RESTRICTED
PE RMT777 CL(JESINPUT) ID(RMT777)
```

c) Ensure that a `FACILITY`-Class profile exists in the format `RJE.RMTnnnn` where `nnn` identifies the remote number.




A command example is shown here:

```
RDEF FACILITY RJE.RMT777 UACC(NONE) OWNER(ADMIN) DATA('COMPLY WITH ZJES0011
FOR RJE 777')
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223756 Rule ID: SV-223756r604139_rule STIG ID: RACF-JS-000120 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9 UNIX System Services

This section describes the UNIX System Services recommendations.

9.1 Ensure that z/OS UNIX SURROGAT resources are protected (Automated)

Profile Applicability:

- Level 1

Description:

Resources in the SURROGAT class that start with "BPX." protect the ability to switch to another identity without providing an authenticator. Servers do this programmatically to run under the identity of their clients, and users can issue the shell 'su' command to switch to another identity. These are sensitive functions that must be protected and logged, and must be used only by servers, not humans.

Rationale:

Improper protection of BPX SURROGAT resources can result in unintended privilege escalation and loss of accountability.

Audit:

All BPX SURROGAT profiles should specify a default (universal) access of NONE. There are several ways this can be checked, including manually, or by using tooling such as reports and queries against RACF Database Unload output, or by inspecting the results of the RACF_SENSITIVE_RESOURCES Health Check. To check manually, issue the SEARCH command to locate all relevant profiles:

```
SEARCH CLASS(SURROGAT) MASK(BPX)
```

For each profile, check the universal access and logging options:

```
RLIST SURROGAT BPX.SRV.userID
```

In the command output, make sure the value under the UNIVERSAL ACCESS heading is NONE.

Verifying that only server user IDs have permission to BPX SURROGAT profiles is a procedural effort.

Remediation:

RACF rules for all BPX.SRV.userid SURROGAT resources must specify a default access of NONE

A sample is provided here:

```
RALTER SURROGAT BPX.SRV.userID UACC(NONE)
```

RACF access lists for all BPX.SRV.userid SURROGAT resources must restrict access to system software processes (e.g., web servers) that act as servers under z/OS UNIX.

Default Value:

When a SURROGAT profile is defined, the default access is NONE.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223844 Rule ID: SV-223844r604139_rule STIG ID: RACF-US-000070 Severity: CAT II

Additional Information:

[Defining Servers Process Users Without Passwords or Password Phrases](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.2 Ensure that resources protecting superuser capabilities in the UNIXPRIV class are protected (Automated)

Profile Applicability:

- Level 1

Description:

Resources in the UNIXPRIV class that start with "SUPERUSER." protect the various capabilities granted to a user with UID(0). By defining profiles in the UNIXPRIV class, you can avoid assigning UID(0) to users by specifically granting certain superuser privileges with a high degree of granularity. This allows you to minimize the number of assignments of superuser authority at your installation and reduces your security risk.

Rationale:

UID(0) generally provides too much authority and presents a separation of duties issue, especially for human users. UNIXPRIV can be used to implement Least Privilege for UNIX superuser authorities.

Audit:

All SUPERUSER UNIXPRIV profiles should specify a default (universal) access of NONE.

There are several ways this can be checked, including manually, or by using tooling such as reports and queries against RACF Database Unload output, or by inspecting the results of the RACF_SENSITIVE_RESOURCES Health Check.

To check manually, issue the SEARCH command to locate all relevant profiles:

```
SEARCH CLASS (UNIXPRIV) MASK (SUPERUSER)
```

For each profile, check the universal access and logging options:

```
RLIST UNIXPRIV SUPERUSER.FILESYS
```

In the command output, make sure the value under the `UNIVERSAL ACCESS` heading is NONE.

Remediation:

Specify a default access of NONE and refresh the UNIXPRIV class:

```
RALTER UNIXPRIV SUPERUSER.FILESYS UACC (NONE)  
SETOPTS RACLIST (UNIXPRIV) REFRESH
```

Default Value:

When a UNIXPRIV profile is defined, the default access is NONE.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223838 Rule ID: SV-223838r604139_rule STIG ID: RACF-US-000010 Severity: CAT I

Additional Information:

1. [Using UNIXPRIV class profiles](#)
2. [Using UNIXPRIV class profiles to manage z/OS UNIX privileges](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.3 Ensure that general users are not allowed to change their file ownership (Automated)

Profile Applicability:

- Level 1

Description:

By default, only superusers can change the ownership of any file to any UID or GID on the system, and general users can only change the group ownership of files that they own, and only to one of their own associated GIDs. However, by defining a profile called CHOWN.UNRESTRICTED in the UNIXPRIV class, selected users can be permitted to transfer ownership of files they own to any UID or GID on the system. This is a less secure configuration.

Rationale:

Only highly trusted users should be allowed to change UNIX file ownership.

Audit:

Look for the existence of the CHOWN.UNRESTRICTED profile in the UNIXPRIV class. It must be a discrete profile.

```
RLIST UNIXPRIV CHOWN.UNRESTRICTED ALL
```

Remediation:

Delete the profile and refresh the UNIXPRIV class.

```
RDELETE UNIXPRIV CHOWN.UNRESTRICTED  
SETROPTS RACLIST (UNIXPRIV) REFRESH
```

Default Value:

RACF does not allow general users to change file ownership to another user, or to a group to which they are not connected.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223838 Rule ID: SV-223838r604139_rule STIG ID: RACF-US-000010 Severity: CAT I

Additional Information:

[Allowing z/OS UNIX users to change file ownerships](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.4 Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted (Automated)

Profile Applicability:

- Level 1

Description:

A user with the RESTRICTED attribute cannot access RACF-protected resources by default mechanisms: the universal access of a profile, ID(*) in an access list, or the global access table. However, this restriction does not automatically apply to UNIX files.

Rationale:

RESTRICTED users may be able to access information they are not intended to have, by virtue of a file's 'other' permission bits.

Audit:

Look for the existence of the RESTRICTED.FILESYS.ACCESS profile in the UNIXPRIV class.

```
RLIST UNIXPRIV CHOWN.UNRESTRICTED ALL
```

Remediation:

Define the profile and refresh the UNIXPRIV class.

```
RDEFINE UNIXPRIV RESTRICTED.FILESYS.ACCESS UACC(NONE)  
SETROPTS RACLIST(UNIXPRIV) REFRESH
```




Default Value:

RACF allows RESTRICTED users to access UNIX files by virtue of the 'other' bits.

Additional Information:

1. [Defining RESTRICTED user IDs](#)
2. [Controlling access to file system resources for restricted users](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.5 Ensure that newly assigned UIDs and GIDs are unique values (Automated)

Profile Applicability:

- Level 1

Description:

When users and groups share UIDs and GIDs, respectively, they are essentially the same entity to the UNIX kernel.

Rationale:

Sharing ids can result in unintended file access and a loss of accountability. Reverse mapping to a user ID or group name does not yield a consistent or predictable result (with the exception of UID 0) which can lead to confusion in displays such as the output of an 'ls' command. The only value that should ever be shared is a UID of 0, which is often required by different daemons and servers.

Impact:

Administrators will need to know that the SHARED keyword must be specified when assigning a value, such as UID(0), that is already in use. They will require READ access to SHARED.IDS in order to do so.

Audit:

Look for the existence of the SHARED.IDS profile in the UNIXPRIV class.

```
RLIST UNIXPRIV SHARED.IDS ALL
```

Remediation:

Define the profile and refresh the UNIXPRIV class.

```
RDEFINE UNIXPRIV SHARED.IDS UACC(NONE)
SETROPTS RACLIST(UNIXPRIV) REFRESH
```




Default Value:

RACF does not prevent assignment of a UNIX ID that is already in use.

Additional Information:

[Controlling the use of shared UNIX identities](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. |  |  |  |

9.6 Ensure that z/OS UNIX user accounts are defined (Automated)

Profile Applicability:

- Level 1

Description:

User IDs, groups, and started tasks that use z/OS UNIX facilities are defined to RACF with an OMVS segment containing attributes such as UID and GID.

Rationale:

If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Audit:

Verify that each z/OS UNIX user's OMVS segment in their USER profile adheres to the following:

1. A unique UID number (except for UID(0) users)
2. A unique HOME directory (except for UID(0) and other system task accounts)
3. Shell program specified as "/bin/sh", "/bin/tcsh", "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

NOTE: RACF ships a set of sample reports based on the output of IRRDBU00 (the RACF data base unload utility) in the SYS1.SAMPLIB member named IRRICE. The report named "UIDS" searches for shared UID values.

Remediation:

The systems programmer will verify that each user account is defined as specified below:

NOTE: This check only applies to users of z/OS UNIX (i.e., users with an OMVS profile defined).

1. A unique UID number (except for UID(0) users)
2. A unique HOME directory (except for UID(0) and other system task accounts)
3. Shell program specified as "/bin/sh", "/bin/tcsh", "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

Default Value:

A user does not have an OMVS segment, and UIDs can be shared.




References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223859 Rule ID: SV-223859r604139_rule STIG ID: RACF-US-000220 Severity: CAT II

Additional Information:

[Using the DFSORT ICETOOL](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. |  |  |  |

9.7 Ensure that RACF Classes required to secure the z/OS UNIX environment are active (Automated)

Profile Applicability:

- Level 1

Description:

The FACILITY, SURROGAT, and UNIXPRIV class support profiles used to secure the z/OS UNIX (OMVS) environment.

UNIXPRIV class profiles are used to manage certain system privileges that are typically associated with z/OS UNIX superuser authority. By defining UNIXPRIV class profiles, certain individual superuser privileges can be granted to users who do not have superuser authority. This reduces the security risks associated with assigning full superuser authority to users.

SURROGAT class profiles are only needed if there are servers (e.g., a web server) running in the z/OS UNIX environment that must be able to act with the security context of a client and that client does not supply a password or other authenticator for RACF.

FACILITY class profiles are used by a variety of IBM components including UNIX System Services (OMVS). BPX prefixed profiles in this class are critical to the proper security of the z/OS UNIX environment.

Rationale:

Without these classes being in active, system integrity can be compromised.

Audit:

The RACF command

```
SETROPTS LIST
```

will show the status of RACF controls including the list of active classes.

To verify that these classes are active, look for the output line `ACTIVE CLASSES =` and inspect the alphabetized list for `SURROGAT`, `UNIXPRIV`, and `FACILITY`.

Remediation:

Ensure that the required classes are active:

```
SETROPTS CLASSACT(FACILITY SURROGAT UNIXPRIV)
```




Default Value:

The classes are not active.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223850 Rule ID: SV-223850r604139_rule STIG ID: RACF-US-000130 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.8 Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed (Automated)

Profile Applicability:

- Level 1

Description:

RACF provides the ability to load certain classes of profiles into memory for better performance with the SETROPTS RACLIST command. For some classes, RACLISTing is required, but it does not happen automatically.

UNIXPRIV class profiles are used to manage certain system privileges that are typically associated with z/OS UNIX superuser authority. By defining UNIXPRIV class profiles, certain individual superuser privileges can be granted to users who do not have superuser authority. This reduces the security risks associated with assigning full superuser authority to users.

SURROGAT class profiles are only needed if there are servers (e.g., a web server) running in the z/OS UNIX environment that must be able to act with the security context of a client and that client does not supply a password or other authenticator for RACF.

FACILITY class profiles are used by a variety of IBM components including UNIX System Services (OMVS). BPX prefixed profiles in this class are critical to the proper security of the z/OS UNIX environment.

Rationale:

Without these classes being RACLISTed, system integrity can be compromised.

Audit:

The RACF command

```
SETROPTS LIST
```

will show the status of RACF controls including the list of RACLISTed classes.

To verify that these classes are RACLISTed, look for the output line `SETR RACLIST CLASSES =` and inspect the alphabetized list for `SURROGAT`, `UNIXPRIV`, and `FACILITY`.

Remediation:

Ensure that the required classes are RACLISTed:

```
SETROPTS RACLIST(FACILITY SURROGAT UNIXPRIV)
```




Default Value:

The classes are not RACLISTed.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022 Vul ID: V-223850 Rule ID: SV-223850r604139_rule STIG ID: RACF-US-000130 Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.9 Ensure that the user account for the z/OS UNIX kernel (OMVS) is defined to the security database (Automated)

Profile Applicability:

- Level 1

Description:

User identifiers (RACF user IDs), groups, and started tasks that use z/OS UNIX facilities are defined to a RACF with attributes including UID and GID. If these... attributes are not correctly defined, data access or command privilege controls could be compromised.

Rationale:

The OMVS (Unix System Services) Kernel must be define with only the required Unix system services attributes, and prevented to access online z/OS facilities (TSO, CICS, ...)

Impact:

If compromised, without the proper attributes, the OMVS Kernel address space user might be used to access z/OS resources.

Audit:

The recommended attributes can be verified using the following command:

```
LU OMVSKERN TSO
LU OMVSKERN CICS
LU OMVSKERN OMVS
```

The output of the `LU OMVSKERN TSO` command should include:

```
NO TSO INFORMATION
```

The output of the `LU OMVSKERN CICS` command should include:

```
NO CICS INFORMATION
```

The output of the `LU OMVSKERN OMVS` command should include:

```
UID= 0000000000
HOME= /
PROGRAM= /bin/sh
```

Remediation:

If the output of the `LU OMVSKERN TSO` command has a TSO segment:

```
ALU OMVSKERN NOTSO
```

If the output of the `LU OMVSKERN CICS` command has a CICS segment:

```
ALU OMVSKERN NOCICS
```



If the output of the `LU OMVSKERN OMVS` command are not consistent with the recommendation:

```
ALU OMVSKERN OMVS (OMVS (UID(0) HOME('/') PROGRAM('/bin/sh'))
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223859 Rule ID: SV-223859r604139_rule STIG ID: RACF-US-000220
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|---|---|
| v8 | 5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | |  |  |

9.10 Ensure that z/OS UNIX automount configuration files are protected (Automated)

Profile Applicability:

- Level 1

Description:

Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls, in particular, the automount facility. . The automount facility can automatically mount file systems at the time they are accessed, and also unmount them later. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Rationale:

The parameters of the autmount facility should be set so they are securely mounted by the automount facility, and the users prevented to execute any file from a file-system using the user of the unix user or group owner other than that file. If not set, these parameters would allow a user to elevate their rights.

Audit:

Review the logical parmlib data sets, example: SYS1.PARMLIB(BPXPRMxx), for the following FILESYSTYPE entry:

| |
|--|
| FILESYSTYPE TYPE(AUTOMNT) ENTRYPPOINT(BPXTAMD) |
|--|

If the above entry is not found or is commented out in the BPXPRMxx member(s), this is NOT APPLICABLE.

Remediation:

Review the settings in /etc/auto.master and /etc/mapname for z/OS UNIX security parameters and ensure that the values conform to the specifications below.

The /etc/auto.master HFS file (and the use of Automount) is optional.

The setuid parameter and the security parameter have a significant security impact. For this reason, these parameters must be explicitly specified and not be allowed to default. Each MapName file will specify the `setuid NO` and `security YES` statements for each automounted directory.

If there is a deviation from the required values, documentation must exist for the deviation.




`Security NO` disables security checking for file access. Security NO is only allowed on test and development domains.

`Setuid YES` allows a user to run under a different UID/GID identity. Justification documentation is required to validate the use of setuid YES.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223854 Rule ID: SV-223854r604139_rule STIG ID: RACF-US-000170
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.11 Ensure that z/OS UNIX security parameters in /etc/inetd.conf are configured (Automated)

Profile Applicability:

- Level 1

Description:

Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. The Unix services are controlled in /etc/inetd.conf and non-essential and potentially non-secure services must be disabled. The parameters impact HFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Rationale:

The /etc/inetd.conf file determine if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures. Some non-essential services can potentially give remote access to attackers (like remote code execution, ...) and must be disabled.

Audit:

Review the settings in `/etc/inetd.conf` file determine if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures.

The following services must be disabled in `/etc/inetd.conf` unless justified and documented:

```
RESTRICTED NETWORK SERVICES
Service Port
Chargen 19
Daytime 13
Discard 9
Echo 7
Exec 512
finger 79
shell 514
time 37
login 513
smtp 25
timed 525
nameserver 42
systat 11
uucp 540
netstat 15
talk 517
qotd 17
tftp 69
```

Remediation:

Review the settings in `/etc/inetd.conf` file determine if every entry in the file represents a service that is actually in use. Services that are not in use must be disabled to reduce potential security exposures.




The following services must be disabled in `/etc/inetd.conf` unless justified and documented:

```
RESTRICTED NETWORK SERVICES
Service Port
Chargen 19
Daytime 13
Discard 9
Echo 7
Exec 512
finger 79
shell 514
time 37
login 513
smtp 25
timed 525
nameserver 42
systat 11
uucp 540
netstat 15
talk 517
qotd 17
tftp 69
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide: Version 8, Release: 6
Benchmark Date: 27 Jan 2022
2. Vul ID: V-223855 Rule ID: SV-223855r604139_rule STIG ID: RACF-US-000180
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

9.12 Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured (Automated)

Profile Applicability:

- Level 1

Description:

This is a setting in IEASYSxx parmlib member to state which BPXPRMxx to use to configure Unix system services. Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls.

Rationale:

The parameters impact ZFS data access and operating system services. Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Audit:

The parameter is specified as `OMVS=xx` or `OMVS=(xx,xx,...)` in the `IEASYSxx` member.

NOTE: If the OMVS statement is not specified, `OMVS=DEFAULT` is used. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server TCP/IP will not run.




Remediation:

Assure that OMVS settings are not defaulting with the `OMVS=(xx,xx)` parameter set.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223851 Rule ID: SV-223851r604139_rule STIG ID: RACF-US-000140
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

9.13 Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are set for security (Automated)

Profile Applicability:

- Level 1

Description:

Parameter settings in PARMLIB member BPXPRMxx and /etc specify values for z/OS UNIX security controls.

Rationale:

The parameters in BPXRPMxx and /etc impact data access and operating system services.

Impact:

Undesirable values can allow users to gain inappropriate privileges that could impact data integrity or the availability of some system services.

Audit:

Review the logical PARMLIB data sets, example: SYS1.PARMLIB (BPXPRMxx) , for the following UNIX Parameter Keywords and Values:

| Parameter | Keyword | Value |
|------------------|--|-------------------|
| SUPERUSER | BPXROOT | |
| TTYGROUP | TTY | |
| STEPLIBLIST | /etc/steplib | |
| USERIDALIASTABLE | Will not be specified. | |
| ROOT | SETUID | will be specified |
| MOUNT | NOSETUID | |
| SETUID | (for Vendor-provided files) | SECURITY |
| STARTUP_PROC | OMVS | |
| UMASK | specify that other write bits are not ON | |

The current runtime parameters can be checked with the commands:

| |
|----------|
| D OMVS,O |
| D OMVS,F |

Remediation:

Review the logical PARMLIB data sets, example: SYS1.PARMLIB (BPXPRMxx) , for the following UNIX Parameter Keywords and Values:

```
Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST /etc/steplib
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID
SETUID (for Vendor-provided files)SECURITY
STARTUP_PROC OMVS
UMASK specify that other write bits are not ON
```




Most of runtime parameters can be dynamically changed with z/OS commands like:

```
SET OMVS=(XX,XX)
SETOMVS parameter=value
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223852 Rule ID: SV-223852r604139_rule STIG ID: RACF-US-000150
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

9.14 Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access (Automated)

Profile Applicability:

- Level 1

Description:

With z/OS UNIX a file owner or a security auditor can specify if auditing is turned on or off, and when audit records should be written for a directory or a file: for successful accesses, failed accesses, or for all accesses. Sensitive files or directories access should be audited. The permissions bits also set access permissions for three classes: owner, group, and other. Sensitive files access must be restricted.

Rationale:

Sensitive configuration files or logs must be restricted to authorized personnel and audited for system integrity. If not audited, uncontrolled modifications to sensitive configuration files or logs would not be detected.

Audit:

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

```
7 rwx (least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)
```

The possible audit bits settings are as follows:

- "f log" for failed access attempts
- "a log" for failed and successful access
- no auditing

The permissions bits and audit bits for a unix file or all the files from a directory can be listed by the command:

```
ls -W [pathname]
```


Remediation:

The permissions bits for a unix file can be modified by the command:

```
chmod mode pathname
```




The audit bits for a unix file can be modified by the command:

| File | Recommended permission bits | Recommended |
|-----------------------------|-----------------------------|-------------|
| audit attributes | | |
| /usr/lpp/tcpip/sbin/syslogd | 1740 | rwxf |
| /etc/syslog.conf | 0744 | w=sf,rx+f |
| /etc/hosts | 0744 | w=sf,rx+f |
| /etc/protocol | 0744 | w=sf,rx+f |
| /etc/resolv.conf | 0744 | w=sf,rx+f |
| /etc/services | 0744 | w=sf,rx+f |
| /usr/lpp/tcpip/bin | 0755 | w=sf,rx+f |
| /usr/lpp/tcpip/sbin | 0755 | w=sf,rx+f |

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223845 Rule ID: SV-223845r604139_rule STIG ID: RACF-US-000080
3. Severity: CAT II
4. Vul ID: V-223846 Rule ID: SV-223846r604139_rule STIG ID: RACF-US-000090
5. Severity: CAT II
6. Vul ID: V-223840 Rule ID: SV-223840r604139_rule STIG ID: RACF-US-000030
7. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.15 Ensure that BPX resources are protected (Automated)

Profile Applicability:

- Level 1

Description:

The RACF FACILITY class profiles starting with BPX are protecting sensitive Unix System Services capabilities and must be protected.

Rationale:

z/OS UNIX RACF-defined resources, starting with BPX. in the FACILITY class consist of sensitive capabilities including SUPERUSER, daemon, and numerous file manipulation privileges.

Impact:

Missing or inaccurate protection of these resources could allow a user to access sensitive data, modify or delete data and operating system controls, or issue commands that could negatively impact system availability.

Audit:

Review the following items for the FACILITY resource class:

1. RACF rules for the BPX.** resource specify a default access of NONE.
2. There are no RACF user access to the BPX.** resource.
3. There is no RACF rule for BPX.SAFFASTPATH defined.
4. RACF rules for each of the BPX resources specify a default access of NONE.
5. RACF rules for each of the BPX resources restrict access to appropriate system tasks or systems programming personnel.

Remediation:




Assure the following are true:

1. RACF rules for the BPX.** resource specify a default access of NONE.
2. There are no RACF user access to the BPX.** resource.
3. There is no RACF rule for BPX.SAFFASTPATH defined.
4. RACF rules for each of the BPX resources specify a default access of NONE.
5. RACF rules for each of the BPX resources restrict access to appropriate system tasks or systems programming personnel.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223839 Rule ID: SV-223839r767099_rule STIG ID: RACF-US-000020
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.16 Ensure that security parameters in etc/profile are configured (Automated)

Profile Applicability:

- Level 1

Description:

The /etc/profile file is the system-wide profile for the z/OS shell users. It contains environment variables and commands used by most shell users. Some variables and commands in a secure system.

Rationale:

When users are using Unix System Services through a shell, we must ensure that specific variables are set and specific commands are issued.

Impact:

If the variables are not set or the commands not executed, the system security can be compromised.

Audit:

The content of the configuration file /etc/profile is listed with the following command:

```
cat /etc/profile
```

It must contain the following entries:

```
umask 077  
readonly LOGNAME
```

Remediation:




If not as required, the /etc/profile following entries must be modified/created

```
umask 077  
readonly LOGNAME
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223842 Rule ID: SV-223842r604139_rule STIG ID: RACF-US-000050
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

9.17 Ensure that security commands in /etc/rc are safe (Automated)

Profile Applicability:

- Level 1
- Level 2

Description:

The /etc/rc file contains customization commands for z/OS UNIX System Services Application Services. Part of these commands are changing files authorization bits and might change auditing options.

Rationale:

Sensitive configuration files or logs must be restricted to authorized personnel and audited for system integrity.text and must not be changed by application services customization commands.

Audit:

Check the content of /etc/rc

If any `chmod` or `chaudit` command target sensitive files (see 1.1.12), they should be removed or changed to the recommended authorization bits/audit attributes.

```
cat /etc/rc
```




Remediation:

Remove/Change the non-conforming lines from the script.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

9.18 Ensure that the BPXROOT user account is configured (Manual)

Profile Applicability:

- Level 1

Description:

The z/OS Unix System Services function “setuid” can be used to change the UID of the process. When the UID requested is UID=0, the user set as SUPERUSER in BPXPRMxx is used. The default user is BPXROOT.

Rationale:

The BPXROOT user must be defined with the correct attributes to the setuid function can be securely used. If these attributes are not correctly defined, data access or command privilege controls could be compromised.

Audit:

The BPXROOT user OMVS segment must be defined with:

```
UID(0)
HOME('/')
PROGRAM('/bin/sh')
```

Additionally, the BPXROOT user should not have access to the BPX.DAEMON profile in the FACILITY class.

```
LU BPXROOT OMVS
RL FACILITY BPX.DAEMON ALL
```



Remediation:

```
ALU BPXROOT OMVS(OMVS(UID(0) HOME('/') PROGRAM('/bin/sh')))
PE BPX.DAEMON CLASS(FACILITY) ID(BPXROOT) DELETE
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223860 Rule ID: SV-223860r604139_rule STIG ID: RACF-US-000230
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|------|---|---|
| v8 | 5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | |  |  |

9.19 Ensure that each RACF group for UNIX is defined with a unique GID (Automated)

Profile Applicability:

- Level 1

Description:

When groups share GIDs, they are essentially the same entity to the UNIX kernel.

Rationale:

Sharing GIDs can result in unintended file access and a loss of accountability. Reverse mapping to a group name does not yield a consistent or predictable result, which can lead to confusion in displays such as the output of an 'ls' command.

Audit:

Search for instances of shared GIDs across the OMVS segments of group profiles. Note that RACF ships a set of sample reports based on the output of IRRDBU00 (the RACF data base unload utility) in the SYS1.SAMPLIB member named IRRICE. The report named "GIDS" searches for shared UID values.

Remediation:




Assign a unique value. Be sure to change group ownership of existing UNIX files accordingly. The following command can locate files owned by a GID (88, in this example):

```
Find / -group 88
```

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223857 Rule ID: SV-223857r767121_rule STIG ID: RACF-US-000200
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. |  |  |  |

9.20 Ensure that data sets used as step libraries in /etc/steplib are configured (Automated)

Profile Applicability:

- Level 1

Description:

The STEPLIBLIST parameter specifies the pathname of the HFS file that contains the list of MVS data sets that are used as step libraries for programs that have the set-user-id or set group id permission bit set. The use of STEPLIBLIST is at the site's discretion, but if used the value of STEPLIBLIST should be /etc/steplib. All update and alter access to the MVS data sets in the list will be logged and only systems programming personnel should be authorized to update the data sets.

Rationale:

Insufficient protection of these data sets can cause the environment to become compromised.

Audit:

UPDATE access to the DATASET profile protecting each data set name in /etc/steplib must be restricted to systems programming personnel. All accesses of UPDATE or higher must be logged.

Remediation:

Modify the profile(s) to restrict access to system programmers, and to log accesses:

```
ALTDS D <dataset-profile-name> UACC(NONE) AUDIT(ALL(UPDATE))
```




Default Value:

Only failed accesses are logged.

References:

1. IBM z/OS RACF Security Technical Implementation Guide :: Version 8, Release: 6 Benchmark Date: 27 Jan 2022
2. Vul ID: V-223849 Rule ID: SV-223849r604139_rule STIG ID: RACF-US-000120
3. Severity: CAT II

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.21 Ensure that ability to switch into superuser mode is restricted (Automated)

Profile Applicability:

- Level 1

Description:

When a user switches into superuser mode (for example, by issuing the 'su' command in the shell) they operate with an effective UID of 0. That is, they are as privileged as if they were assigned UID(0) in their OMVS segment.

Rationale:

Granting access to BPX.SUPERUSER should be viewed to be as sensitive as explicitly assigning UID(0). Erroneous access to BPX.SUPERUSER can result in complete compromise of the system.

Audit:

Use the `RLIST` command to display the `BPX.SUPERUSER` profile.

```
RLIST FACILITY BPX.SUPERUSER ALL
```

In the command output, make sure the value under the `UNIVERSAL ACCESS` heading is `NONE`

Remediation:




Set the universal access to `NONE` and refresh the `FACILITY` class:

```
RALTER FACILITY BPX.SUPERUSER UACC (NONE)  
SETROPTS RACLIST(FACILITY) REFRESH
```

Default Value:

Profiles in the `FACILITY` class have a `UACC` value of `NONE` when defined.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.22 Ensure file permission for universal write is restricted (Automated)

Profile Applicability:

- Level 1

Description:

z/OS zFS datasets contains z/OS Unix file systems data. If not protected these datasets can be modified, hindering system security.

Rationale:

Z/OS zFS datasets contains the files from the z/OS Unix file systems along with the unix attributes controlling security.

Audit:

Verify that the zFS dataset protecting profile prevent any universal access greater than read (NON preferred).


```
LD DATASET ( 'ZFS.DATASET' )
```

Remediation:

Change the UACC attribute to NONE

```
ALTDSD 'ZFS.DATASET' UACC (NONE)
```

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.23 Ensure USS Telnet server is not active (Automated)

Profile Applicability:

- Level 1

Description:

Running the USS Telnet server is a security concern as telnet data flow is not encrypted. SSH is recommended.

Rationale:

Using an unencrypted network protocol results in clear text passwords being sent across the network connection.



Audit:

The `otelnetd` server should not be activated through the `inetd` daemon (through `/etc/inetd.conf`) or permitted in the list of TCPIP services (`/etc/services` or `hlq.ETC.SERVICES`)

Remediation:

Remove the `otelnet` entry from `/etc/inetd.conf` and the `otelnetd` entry from `/etc/services` (or `hlq.ETC.SERVICES` dataset).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |

9.24 Ensure rlogin is not active (Manual)

Profile Applicability:

- Level 1

Description:

The rlogin command enables log in to a remote system and navigate through the remote file system and manipulate its contents, copy files, or execute remote commands.

Rationale:

rlogin server processing is operating in clear text and therefore should be prevented to start.



Audit:

The rlogind server should not be activated through the inet daemon (through /etc/inetd.conf) or permitted in the list of TCPIP services (/etc/services or hlq.ETC.SERVICES).

Remediation:

Remove the login entry from /etc/inetd.conf and the login entry from /etc/services (or hlq.ETC.SERVICES dataset).

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|------|---|---|
| v8 | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | |  |  |

9.25 Ensure changes to UNIX file security are logged (Manual)

Profile Applicability:

- Level 1

Description:

By default, UNIX security attribute (e.g. owner, permission bits) changes are not logged in SMF Type 80 records. These changes should be logged, just as changes to RACF profiles should be logged.

Rationale:

In the absence of SMF Type 80 records for UNIX file security attribute changes, it is more difficult to debug authorization problems and investigate potential attacks. Enabling logging for security changes provides a historical record of security changes and allows for ICH408I violation messages to be sent to the security console when an unauthorized person attempts to change security attributes.

Audit:

Verify that all attempts to change UNIX file security attributes are logged. From the TSO command line, enter the following command from a user ID with the AUDITOR or ROAUDIT attribute:

```
SETROPTS LIST
```

Locate the line starting with:

```
LOGOPTIONS "ALWAYS" CLASSES =
```

Inspect the alphabetized list for the presence of the FSSEC class.

Remediation:

Enable logging for all attempts to change UNIX file security attributes. From the TSO command line, enter the following command from a user ID with the AUDITOR attribute:

```
SETROPTS LOGOPTIONS (ALWAYS (FSSEC) )
```




Default Value:

Changes to security attributes (or failed attempts to do so) are not logged.

Additional Information:

[Auditing for z/O UNIX System Services](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |

9.26 *Ensure that programs cannot execute from the /tmp directory (Automated)*

Profile Applicability:

- Level 1

Description:

By default, programs and scripts can be run from within any file system in the hierarchy. This ability should be restricted from within the /tmp directory. The FSEXEC class can be used to prevent file execution from an individual file system regardless of permission bits, file ownership, or even superuser privilege.

Rationale:

When an attacker gains access to UNIX, their first action is often to run a script to detect system vulnerabilities. The /tmp directory is often used for this purpose because all users, by necessity, can typically create files in this directory.

Impact:

An additional access check is performed whenever a file is opened for execute access.

Audit:

Verify that file execution is not allowed in the `/tmp` directory. The `/tmp` directory must be protected by a profile in the `FSEXEC` class, and the `FSEXEC` class must be active and `RACLISTed`.

From the TSO command line, enter the following command from a user ID with the `SPECIAL`, `AUDITOR` or `ROAUDIT` attribute:

```
SETROPTS LIST
```

Locate the line starting with:

```
ACTIVE CLASSES =
```

Inspect the alphabetized list for the presence of the `FSEXEC` class.

Locate the line starting with:

```
SETR RACLIST CLASSES =
```

Inspect the alphabetized list for the presence of the `FSEXEC` class.

Identify the file system that contains the `/tmp` directory. From the shell, issue the command:

```
df /tmp
```

You will see output such as:

| | | | | |
|-------------|------------|-------------|-------|-----------|
| # df /tmp | | | | |
| Mounted on | Filesystem | Avail/Total | Files | Status |
| /SYSTEM/tmp | (/tmp) | 81688/81920 | 10211 | Available |

In the `Filesystem` column, the name of the file system is identified. For most file systems, the value is a data set name. However, the `/tmp` directory often uses the `tfs` file system, which is not backed by a data set. To see if the resource is defined to the `FSEXEC` class, issue the following command:

```
RLIST FSEXEC /tmp
```

In the command output, make sure the value under the `UNIVERSAL ACCESS` column is `NONE`

Remediation:

Protect `/tmp` in the `FSEXEC` class and activate and `RACLIST` the class.

From the TSO command line, enter the following command from a user ID with the `SPECIAL` attribute:

```
RDEFINE FSEXEC /tmp UACC(NONE)  
SETROPTS CLASSACT(FSEXEC) RACLIST(FSEXEC)
```




Default Value:

The `FSEXEC` class is not active, and files can be executed from `/tmp`.

Additional Information:

[Restricting execute access in a zFS or TFS file system](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.27 Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier (Manual)

Profile Applicability:

- Level 1

Description:

A naming convention is generally established when allocating new zFS user file systems for a UNIX user to have as their home directory. If the high-level qualifier for this data set is the user's RACF user ID, then the user has read and write access to it outside of the UNIX environment where UNIX authorization checks are not made.

Rationale:

A user can set sensitive file attributes from the traditional MVS environment, and they will be honored within the UNIX environment. This can lead to full compromise of your system.

Audit:

Check the names of the zFS aggregates used for user file systems. The shell `df` command displays all file systems by path name and by zFS data set name.




```
df
```

In the `Filesystem` column, the names of all mounted file systems are identified.

Remediation:

Establish a plan by which to replace these file systems. Modify your provisioning steps (for example, your automount policy) to discontinue the user ID-based naming convention in the high-level qualifier.

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.28 Ensure that daemons are running with z/OS UNIX level security (Automated)

Profile Applicability:

- Level 1

Description:

Running with z/OS UNIX level security ensures that system programmers with UID(0) cannot switch identity to any other z/OS UNIX user without authentication. This capability is restricted to daemon user IDs with READ access to BPX.DAEMON in the FACILITY class.

Rationale:

In contrast, with UNIX level security, anyone with UID(0) or access to BPX.SUPERUSER in the FACILITY class can switch identity to any other z/OS UNIX user without authentication. This violates separation of duties and least privilege.

Impact:

Implementing z/OS UNIX level security requires daemons to be running in a clean address space. This requires additional setup and maintenance to identify programs that are allowed to execute in the daemon address space and define them to RACF program control.

Audit:

Verify that the BPX.DAEMON profile is defined in the FACILITY class and that only daemon user IDs are permitted with READ access.

```
RLIST FACILITY BPX.DAEMON AUTHUSER
```

Remediation:

Establish a plan by which to identify programs that are executed by the daemon application, define them to program control, and then define BPX.DAEMON in the FACILITY class.




Default Value:

UNIX level security is in effect.

Additional Information:

Setting up for daemons - <https://www.ibm.com/docs/en/zos/2.5.0?topic=planning-setting-up-daemons>

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |  |  |  |

9.29 Ensure that servers are running with z/OS UNIX level security (Automated)

Profile Applicability:

- Level 1

Description:

Running with z/OS UNIX level security ensures that system programmers with UID(0) cannot establish thread-level security under any other z/OS UNIX user without authentication. This capability is restricted to server user IDs with READ or UPDATE access to BPX.SERVER in the FACILITY class.

Rationale:

In contrast, with UNIX level security, anyone with UID(0) or access to BPX.SUPERUSER in the FACILITY class can establish thread-level security under any other z/OS UNIX user without authentication. This violates separation of duties and least privilege.

Impact:

Implementing z/OS UNIX level security requires servers to be running in a clean address space. This requires additional setup and maintenance to identify programs that are allowed to execute in the server address space and define them to RACF program control.

Audit:

Verify that the `BPX.SERVER` profile is defined in the `FACILITY` class and that only server user IDs are permitted with `READ` or `UPDATE` access.

```
RLIST FACILITY BPX.SERVER AUTHUSER
```

Remediation:

Establish a plan by which to identify programs that are executed by the server application, define them to program control, and then define `BPX.SERVER` in the `FACILITY` class.




Default Value:

UNIX level security is in effect.

Additional Information:

[Establishing the correct level of security for servers](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |  |  |  |

9.30 Ensure that file systems containing critical data are protected from access using profiles in the FSACCESS class (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Critical data can be stored within zFS file systems. Access to files and directories is controlled by z/OS UNIX mechanisms such as UID(0), file ownership, file permission and access control lists. Using profiles in the FSACCESS class, you can restrict the ability to cross a mount point into a zFS file system to only those explicitly permitted in the profile. This overrides even UID(0) authority. Once you have crossed the mount point, UNIX rules apply when accessing files and directories within that file system.

File systems containing critical data should be protected with an FSACCESS profile.

Rationale:

Access at the mount point level is controlled only by RACF security administrators. This provides a clear separation of duties in the event that you have UID(0) users. It also provides protection against overly permissive access rules in z/OS UNIX made outside the scope of control of the security administrator.

Impact:

Use of the FSACCESS class can cause increased CPU usage in some environments.

Audit:

Make sure that the `FSACCESS` class is active and RACLISTed, as reported by the `SETROPTS LIST` command.

The UNIX shell command named `df` will display a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name.

For each of these, identify the ones that contain critical data.

Using the data set name as a RACF profile name, see if it is covered by an `FSACCESS` profile:

```
RLIST FSACCESS <data-set-name> ALL
```

Remediation:

For each data set containing critical data, define an `FSACCESS` profile (discrete or generic as the nature of the data requires) with the following attributes:

- UACC(NONE)
- No ID(*) on the access list
- Not in WARNING mode
- READ access is restricted to only those who need to access the critical data and to those managing the security of the files and directories within the file system
- All accesses are being logged




Default Value:

The `FSACCESS` class is not active.

Additional Information:

1. [df - Display the amount of free space in the file system](#)
2. [Restricting access to a zFS file system](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|--|---|---|---|
| v8 | 3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

9.31 Ensure that file systems are mounted read-only wherever possible (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Some zFS file systems contain data that is not expected to change. For example, a file system may be dedicated to containing the binary executables of a specific application. You generally do not expect this data to change until the next time you apply service.

Rationale:

Mounting a file system in read-only mode protects against accidental or malicious changes to the data within.

Impact:

None.

Audit:

The UNIX shell command named `df` displays a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name. Using the verbose option, yields additional information, including the mount mode.

```
df -v
```

The mount mode will be displayed as `Read Only` or `Read/Write`




Remediation:

For each `Read/Write`-mounted file system in which you don't expect data to change, plan to remount it in `read-only` mode as application availability allows, and update the `BPXPRMxx` member of `SYS1.PARMLIB` to make the change effective at the next IPL

Additional Information:

1. list text here [df - Display the amount of free space in the file system](#)
2. list text here [mount - Logically mount a file system](#)
3. [unmount - Remove a file system from the file hierarchy](#)
4. [BPXPRMxx \(z/OS UNIX System Services parameters\)](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |  |  |  |

9.32 Ensure that file systems are mounted with set-id files disabled wherever possible (Manual)

Profile Applicability:

- Level 1

Description:

Set-user-ID and set-group-ID files are those containing executables that run under the identity of the file owner rather than the person running the executable. These are often the target of attackers. On the other hand, some applications rely on these types of files to operate as expected. Any file system that is not expected to contain set-id files should be mounted in NOSETUID mode. In this mode, the set-user-ID and set-group-ID bits in the file mode are ignored.

Rationale:

Mounting a file system in NOSETUID mode reduces the attack surface of your zFS file systems.

Impact:

None

Audit:

The UNIX shell command named `df` displays a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name. Using the verbose option, yields additional information, including mount options.

```
df -v
```

The presence of the string `No SUID` indicates the file system is mounted with the `NOSETUID` option. If it is mounted with the default of `SETUID`, no option is displayed.

The shell `find` command can be used to search for occurrences of `set-user-ID` and `set-group-ID` files starting at the path name specified. For example, to see if any `set-id` files exist in the file system mounted on the `/usr/lpp/appx` directory:

```
find /usr/lpp/appx -type f \( -perm -4000 -o -perm -2000 \)
```

Note: The spaces within the parentheses are significant.




Remediation:

For each file system in which you don't expect `set-id` files to exist, plan to remount it with the `NOSETUID` option as application availability allows, and update the `BPXPRMxx` member of `SYS1.PARMLIB` to make the change effective at the next IPL

Additional Information:

1. [df - Display the amount of free space in the file system](#)
2. [find - Find a file that meets specified criteria](#)
3. [mount - Logically mount a file system](#)
4. [unmount - Remove a file system from the file hierarchy](#)
5. [BPXPRMxx \(z/OS UNIX System Services parameters\)](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |  |  |  |

9.33 *Ensure that no file systems are mounted with security disabled (Automated)*

Profile Applicability:

- Level 1

Description:

If a file system is mounted with the NOSECURITY option, everyone has all access to every object in the file system. In a production environment, no file system should be mounted with this option.

Rationale:

Mounting a file system in NOSECURITY mode completely nullifies any access control established within it, opening the data for reading and writing to everyone.

Impact:

None

Audit:

The UNIX shell command named `df` displays a list of the currently mounted file systems, by mount point (UNIX directory path) and data set name. Using the verbose option, yields additional information, including mount options.

```
df -v
```

The presence of the string `No Security` indicates the file system is mounted with the NOSECURITY option. If it is mounted with the default of `SECURITY`, no option is displayed.




Remediation:

For each file system mounted with the NOSECURITY option, plan to remount it without the NOSECURITY option as application availability allows and update the `BPXPRMxx` member of `SYS1.PARMLIB` to make the change effective at the next IPL

Additional Information:

1. [mount - Logically mount a file system](#)
2. [unmount - Remove a file system from the file hierarchy](#)
3. [BPXPRMxx \(z/OS UNIX System Services parameters\)](#)

CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|------------------|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. |  |  |  |

Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 1 | Identification and Authentication | | |
| 1.1 | Password Control | | |
| 1.1.1 | Ensure that the PASSWORD(INTERVAL) SETROPTS value is set to no longer than 90 days (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2 | Ensure that the PASSWORD(HISTORY) SETROPTS value is set to at least 4 (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3 | Ensure that the PASSWORD(RULEn) SETROPTS value(s) is set (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.4 | Ensure that the SETROPTS PASSWORD(MINCHANGE(n)) value will specified a value greater the zero (0) (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5 | Ensure that the PASSWORD(REVOKE) SETROPTS value is specified (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6 | Ensure that the KDFAES algorithm is used to protect passwords in the security database (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7 | Ensure that the PASSWORD(WARNING) SETROPTS value is set (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2 | System Settings | | |
| 1.2.1 | Ensure that Inactive users are revoked (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2 | Ensure that STARTED class is used to assign users to Started Tasks (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.3 | Ensure user propagation is protected with the PROPCNTL class (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.4 | Ensure that Job wait time option is set (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 1.2.5 | Ensure that started tasks defined with the trusted attribute are justified (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.6 | Ensure that the OPERCMDS resource class is ACTIVE and RACLISTed (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.7 | Ensure that CONSOLE resource class is ACTIVE (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.8 | Ensure that FACILITY resource class is ACTIVE and RACLISTED (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.9 | Ensure that inapplicable PPT entries have been invalidated (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.10 | Ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) currently active parmlib data set(s) (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.11 | Ensure that the CONSOLxx members are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.12 | Ensure that no expired digital certificates are used (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.13 | Ensure that RACF RVARYPW are set to non-default values (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3 | User Attributes | | |
| 1.3.1 | Ensure that the use of RACF SPECIAL Attribute is justified (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.2 | Ensure that SYS1.UADS contains only emergency use user IDs (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.3 | Ensure that MCS console user ID(s) is protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.4 | Ensure that all STARTED class profiles specify PROTECTED user IDs (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 2 | Authorization and Access Control Management | | |
| 2.1 | Data Protection | | |
| 2.1.1 | Ensure that Maintenance user IDs are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2 | Ensure that access to active SMF collection files is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3 | Ensure that the WHEN(PROGRAM) SETROPTS value is active (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4 | Ensure that the ICHDSM00 program is protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5 | Ensure that the IRRDPI00 program is protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6 | Ensure that the SETROPTS ERASE value is set to ERASE(ALL) on all systems (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7 | Ensure that the TEMPDSN class is active (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.8 | Ensure the RACF security data sets and all copies are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.9 | Ensure the RACF remote sharing facility files are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.10 | Ensure the RACF parameter library file is protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.11 | Ensure that RACF remote sharing connections use the TCP/IP protocol (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.12 | Ensure that memory and privileged program dumps are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.13 | Ensure that access to system trace datasets is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 2.1.14 | Ensure that access to system backup datasets is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15 | Ensure that access to SYSTEM DUMP data sets is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.16 | Ensure that access to SMF collection offload datasets is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.17 | ENSURE that Temporary Data Sets are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2 | Resource Protection | | |
| 2.2.1 | Ensure that the ability to update system dynamic lists are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2 | Ensure that the GENERIC SETROPTS value is enabled for ACTIVE classes (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3 | Ensure that IEASYMUP resource is protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4 | Ensure that PASSWORD protection for data sets is not used (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5 | Ensure that access to datasets in the PARMLIB concatenation is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6 | Ensure that access to all LPA libraries is controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.7 | Ensure that access to the System Master Catalog is controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.8 | Ensure that access to all APF-authorized objects is controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.9 | Ensure that access to SYS1.SVCLIB is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.10 | Ensure that access to SYS1.IMAGELIB is controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 2.2.11 | Ensure that access to libraries that contain PPT modules is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.12 | Ensure that access to SYS1.NUCLEUS is controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.13 | Ensure that access to all system PROCLIB data sets is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.14 | Ensure that System REXX data set is protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.15 | Ensure that Access to SYS1.LINKLIB is protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.16 | Ensure that access to all system-level product installation libraries is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3 | System Settings | | |
| 2.3.1 | Ensure that the TERMINAL SETROPTS value is set to NONE (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2 | Ensure that the GENCMD SETROPTS value is enabled for ACTIVE classes (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3 | Ensure that the PROTECTALL SETROPTS value is set to FAIL (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4 | User Privilege | | |
| 2.4.1 | Ensure that the assignment of the RACF OPERATIONS attribute is tightly controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2 | Ensure that TSOAUTH resources are restricted to authorized users (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.3 | Ensure that access for Surrogate users is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.4 | Ensure that UID 0 is only assigned to PROTECTED STC IDs (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 2.4.5 | Ensure that started tasks requiring exceptional access rights use the TRUSTED attribute and (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.6 | Ensure that access to Libraries containing EXIT modules is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.7 | Ensure that access to LINKLIST libraries is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.8 | Ensure that access to SYS1.UADS is maintained (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.9 | Ensure that Access to System page data sets (i.e., PLPA, COMMON, and LOCALx) is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.10 | Ensure that MCS consoles access is protected through CONSOLE CLASS profile (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.11 | Ensure that access to CONSOLE resources for users in TSOAUTH resource class is restricted (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.12 | Ensure that access to system user catalogs is controlled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | Logging and Auditing | | |
| 3.1 | Ensure that the command violations are being logged (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2 | Ensure that activity of SPECIAL users are being logged (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3 | Ensure that the AUDIT SETROPTS value is set for all classes (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4 | Ensure that activities of users with the OPERATIONS attribute are logged (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5 | Ensure that Logon statistics are recorded (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 3.6 | Ensure RACF AUDITOR or ROAUDIT privilege is assigned only to users with auditing mission. (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7 | Ensure that effective SMF records collection options are set (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8 | Ensure that an automated process is in place to collect and retain SMF data (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9 | Ensure that Required SMF data record types is collected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10 | Ensure that RACF audit logs is reviewed on a regular basis (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11 | Ensure regular audit of AC=1 modules in APF authorized libraries are conducted (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.12 | Ensure that only supported (vendor) system software is installed and active on the system (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.13 | Ensure all software on your system is supported (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.14 | Implement sensitive z/OS datasets monitoring (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | System Resilience | | |
| 4.1 | Ensure that RACF database is backed up on a scheduled basis (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2 | Ensure that RACF primary and backup databases are isolated (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3 | Ensure sensitive data is encrypted (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | Storage Management | | |
| 5.1 | Ensure that DFSMS is configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 5.2 | Ensure that a very limited number of users can use the Tape Bypass Label Processing (BLP) (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3 | Ensure that Automatic Data Set Protection (ADSP) SETROPTS value is set to NOADSP (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4 | Ensure that DFSMS control data sets are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | Networking | | |
| 6.1 | CSSMTP Recommendations | | |
| 6.1.1 | Ensure CSSMTP Started Task name is configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2 | Ensure CSSMTP Started task(s) is defined to the STARTED resource class. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3 | Ensure AT-TLS protection is enabled for CSSMTP (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4 | Ensure CSSMTP STC data sets are protected. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2 | FTP Recommendations | | |
| 6.2.1 | Ensure FTP Server daemon is configured with proper security parameters (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2 | Ensure startup parameters for the FTP daemon do not allow ANONYMOUS or INACTIVE keywords (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3 | Ensure FTP.DATA configuration statements enforce secure configuration (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.4 | Ensure AT-TLS protection is enabled for the FTP daemon (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.5 | Ensure User exits for the FTP Server are not used without approval (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 6.2.6 | Ensure warning banner for the FTP Server is specified (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.7 | Ensure SMF recording options for the FTP Server are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.8 | Ensure permission and user audit bits for FTP Server are configured. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.9 | Ensure MVS data sets for the FTP Server are protected. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.10 | Ensure FTP Control cards are stored in a secure PDS file (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3 | OpenSSH | | |
| 6.3.1 | Ensure SSH daemon is configured to only use the SSHv2 protocol (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2 | (Optional) Ensure SSH daemon is configured to use FIPS 140-2 compliant cryptographic provider where required (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3 | Ensure SSH daemon is configured with the logon banner (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4 | Ensure SMF recording options for the SSH daemon are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.5 | Ensure SSH daemon is configured to use SAF keyrings for key storage (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4 | Syslogd Recommendations | | |
| 6.4.1 | Ensure Syslog daemon is started at z/OS initialization (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4.2 | Ensure Syslog daemon is secured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.4.3 | Ensure permission and user audit bits for Syslog daemon component are configured. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 6.4.4 | Ensure syslogd archive data sets are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5 | TCP/IP Recommendations | | |
| 6.5.1 | Ensure configuration files for the TCP/IP stack are explicitly specified (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.2 | Ensure TCP/IP stack configuration defined in TCPIP.DATA (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.3 | Ensure Hosts identified by the NSINTERADDR statement are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.4 | Ensure PROFILE.TCPIP configuration statements for the TCP/IP stack are defined (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.5 | Ensure permission and user audit bits for z/OS Unix file system objects that are part of the Base TCP/IP component are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.6 | Ensure access to TCP/IP SAF resources (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.7 | Ensure RACF SERVAUTH resource class is active for TCP/IP resources (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.8 | Ensure Started tasks for the base TCP/IP component are defined securely in RACF (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.5.9 | Ensure MVS data sets for the Base TCP/IP component are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6 | TN3270 Recommendations | | |
| 6.6.1 | Ensure configuration statements for the TN3270E Telnet Server are configured. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6.2 | Ensure VTAM session setup controls for the TN3270E Telnet Server are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6.3 | Ensure Warning banner for the TN3270 Telnet Server is configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 6.6.4 | Ensure AT-TLS protection is enabled for the TN3270 Telnet Server (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6.5 | Ensure SMF recording options for the TN3270 Telnet Server are configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.6.6 | Ensure Startup user account for the z/OS UNIX Telnet Server is defined (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7 | VTAM Recommendations | | |
| 6.7.1 | Ensure VTAM USSTAB definitions are being used for secured terminals (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.7.2 | Ensure System datasets used to support the VTAM network are secured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | Cryptography and Encryption | | |
| 7.1 | ICSF Installation and Configuration | | |
| 7.1.1 | Ensure that all ICSF Installation Datasets are protected. (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2 | Ensure that the ICSF Started Task is protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3 | Ensure CSFINPV2 requires signature verification (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4 | Ensure ICSF is configured to start during IPL (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2 | ICSF Component Configuration | | |
| 7.2.1 | Ensure Crypto Usage Statistics are enabled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2 | Ensure Crypto Key Lifecycle Auditing is enabled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.3 | Ensure Crypto Key Usage Auditing is enabled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4 | Ensure ICSF Key Data Sets have a system backup (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 7.2.5 | Ensure ICSF Master Keys have a backup procedure (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.6 | Ensure all ICSF Key Data Sets are in Common Record Format (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.7 | Ensure all ICSF Key Data Sets are enabled for sysplex sharing (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.8 | Ensure ICSF is running with FIPSMODE enabled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9 | Ensure CCA Operational Keys Are Created with WRAPENH3 Key Wrapping (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3 | ICSF Security Configuration | | |
| 7.3.1 | Ensure CSFSERV class is active (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.2 | Ensure CSFKEYS class is active (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.3 | Ensure CRYPTOZ class is active (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.4 | Ensure the XCSFKEY class is active (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.5 | Ensure ICSF Key Store Policy controls are enabled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.6 | Ensure ICSF Key Datasets are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.7 | Ensure ICSF administrative services are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.3.8 | Ensure ICSF operator commands are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | Job Management JES2 | | |
| 8.1 | JES2 Commands | | |
| 8.1.1 | Ensure that JES2 system commands are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 8.2 | JES2 SPOOL | | |
| 8.2.1 | Ensure that JESSPOOL CLASS is active (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.2.2 | Ensure that JES2 spool resources are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.2.3 | Ensure that JES2 trace resources are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.2.4 | Ensure that JESNEWS resources are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3 | Job Level Protection | | |
| 8.3.1 | Ensure that JESJOBS CLASS is set up (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.2 | Ensure CANCEL JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.3 | Awareness of the ENCRYPT JESJOBS profiles (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.4 | Ensure GROUPREG JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.5 | Ensure HOLD JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.6 | Ensure JOBCCLASS JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.7 | Ensure JOBNFY JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.8 | Ensure MODIFY JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.9 | Ensure PURGE JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.10 | Ensure RELEASE JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 8.3.11 | Ensure REROUTE JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.12 | Ensure SPIN JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.13 | Ensure SPOOLIO JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.14 | Ensure START JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.3.15 | Ensure SUBMIT JESJOBS profiles are protected (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.4 | Enable Encryption of Data Set on SPOOL | | |
| 8.4.1 | Ensure that data sets on SPOOL are encrypted as required (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.4.2 | Require user identification (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.4.3 | Ensure that the JES(BATCHALLRACF) SETROPTS value is set to JES(BATCHALLRACF) (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.4.4 | Ensure that the JES(XBMALLRACF) SETROPTS value is set to JES(XBMALLRACF) (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.5 | Control Access to Data Sets Used by JES2 | | |
| 8.5.1 | Ensure that access (read, update and allocate) to the data sets used by JES2 is controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.5.2 | Ensure that access to any PROCLIB data sets used by JES2 is protected from unintended updates (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.5.3 | Ensure that RACF is called for data sets opened by JES2 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.6 | Device Management | | |
| 8.6.1 | Ensure that JES2 output devices are controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 8.6.2 | Ensure that bypass label processing (BLP=) is not set on any JOBCLASS (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.6.3 | Ensure that use of JES2 input sources are controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.7 | JES2 Networking | | |
| 8.7.1 | Ensure that RJE workstations and NJE nodes are controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 8.7.2 | Ensure that RJE workstations and NJE nodes are controlled (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | UNIX System Services | | |
| 9.1 | Ensure that z/OS UNIX SURROGAT resources are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.2 | Ensure that resources protecting superuser capabilities in the UNIXPRIV class are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.3 | Ensure that general users are not allowed to change their file ownership (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.4 | Ensure that RESTRICTED users cannot access UNIX files to which they are not explicitly permitted (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.5 | Ensure that newly assigned UIDs and GIDs are unique values (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.6 | Ensure that z/OS UNIX user accounts are defined (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.7 | Ensure that RACF Classes required to secure the z/OS UNIX environment are active (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.8 | Ensure that RACF Classes required to secure the z/OS UNIX environment are RACLISTed (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|--|--------------------------|--------------------------|
| | | Yes | No |
| 9.9 | Ensure that the user account for the z/OS UNIX kernel (OMVS) is defined to the security database (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.10 | Ensure that z/OS UNIX automount configuration files are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.11 | Ensure that z/OS UNIX security parameters in /etc/inetd.conf are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.12 | Ensure that z/OS UNIX OMVS parameters in IEASYSxx are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.13 | Ensure that z/OS UNIX BPXPRMxx parameters in PARMLIB are set for security (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.14 | Ensure that z/OS UNIX permission bits and audit bits are configured to audit sensitive file access (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.15 | Ensure that BPX resources are protected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.16 | Ensure that security parameters in etc/profile are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.17 | Ensure that security commands in /etc/rc are safe (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.18 | Ensure that the BPXROOT user account is configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.19 | Ensure that each RACF group for UNIX is defined with a unique GID (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.20 | Ensure that data sets used as step libraries in /etc/steplib are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.21 | Ensure that ability to switch into superuser mode is restricted (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.22 | Ensure file permission for universal write is restricted (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.23 | Ensure USS Telnet server is not active (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation | | Set Correctly | |
|------------------------------|---|--------------------------|--------------------------|
| | | Yes | No |
| 9.24 | Ensure rlogin is not active (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.25 | Ensure changes to UNIX file security are logged (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.26 | Ensure that programs cannot execute from the /tmp directory (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.27 | Ensure that data sets containing user file systems do not have the user ID as the high-level qualifier (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.28 | Ensure that daemons are running with z/OS UNIX level security (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.29 | Ensure that servers are running with z/OS UNIX level security (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.30 | Ensure that file systems containing critical data are protected from access using profiles in the FSACCESS class (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.31 | Ensure that file systems are mounted read-only wherever possible (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.32 | Ensure that file systems are mounted with set-id files disabled wherever possible (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 9.33 | Ensure that no file systems are mounted with security disabled (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

Appendix: Change History

| Date | Version | Changes for this version |
|--------------|---------|--------------------------|
| May 20, 2022 | 1.0.0 | Published |