The New NIST/DHS Security Controls for z Systems

Presented by Brian Marshall,
Vice President, Research and Development
Vanguard Integrity Professionals

Booth 426

Agenda

- Terms and Terminology
- History of the STIGS
- Categories of STIG Checks
- Anatomy of a STIG
- Anatomy of a CCI
- STIGS of Interest
- Changes since 6.20
- Questions

This is a z System

In General

General Information:

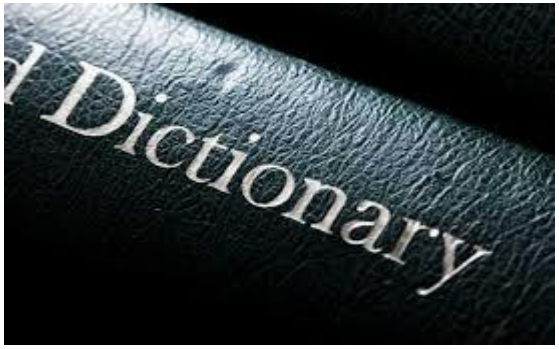
Session will be using the current version of the DISA STIG checklists 6.22 as of this writing. The DISA STIG checklist is generally newer than those posted on the NIST NCP website.

Disclaimers:

- Some of the checks in the checklist may not be applicable to you.
- You may not be able to implement some of the checks/requirements in your environment.
- Some checks are open to interpretation. The presenter does not represent DISA and is only presenting his opinion and observations.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Terms and Terminology



IBM Server Proven

Business Partner IBM

Terms and Terminology

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Defense Information Systems Agency (DISA)

A United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands.

National Institute of Standards and Technology (NIST)

Publishes configuration controls that must be used by each Federal Agency and by all contractors processing data for a federal agency.

Security Technical Implementation Guide (STIG)

A configuration document used to standardized security controls for software and hardware systems. Each **STIG** check in the SRR checklist is mapped to IA Controls defined in **DoD Directive 8500.2.**

Terms and Terminology

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Department of Defense (DoD)

The U.S. federal department charged with coordinating and supervising all agencies and functions of the government relating directly to national security and the United States armed forces.

DoD Directive 8500.1

Requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks **DISA** to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.”

Terms and Terminology

DoD IA Controls

The Defense Information Assurance (IA) program establishes a baseline set of controls to be applied to all DoD information systems. Each control is uniquely named and can be referenced, measured, and reported against throughout the life cycle of a DoD information system.

Security Readiness Review (SRR)

The audit performed at designated sites to review compliance with the **DISA STIGs.**

SRRAUDIT

The name assigned to the **SSR** audit process to validate compliance with the **DISA STIG**s.

DHS

Department of Homeland Security

Terms and Terminology

CCI

Control Correlation Identifiers

Checks

A specific vulnerability test or configuration control. Each Check gets its first few characters from the category of checks it is in.
For example, ACP00282 – Access Control Program (ACP)

Checklist

Refers to the list of **checks** that are to be performed as part of the **SRR**

Checklist Result

Outcome of a check - Open, Not A Finding, Not Reviewed, Not Applicable

Terms and Terminology

Finding Severities

Category I - Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.

Category II - Vulnerabilities that provide information that have a high potential of giving access to an intruder.

Category III - Vulnerabilities that provide information that potentially could lead to compromise.

NCP

National Checklist Program (Part of the NVD)

NVD

National Vulnerability Database (hosted by NIST and DHS)

Terms and Terminology

Vulid

Vulnerability Identification

XCCDF

Extensible Configuration Checklist Description Format

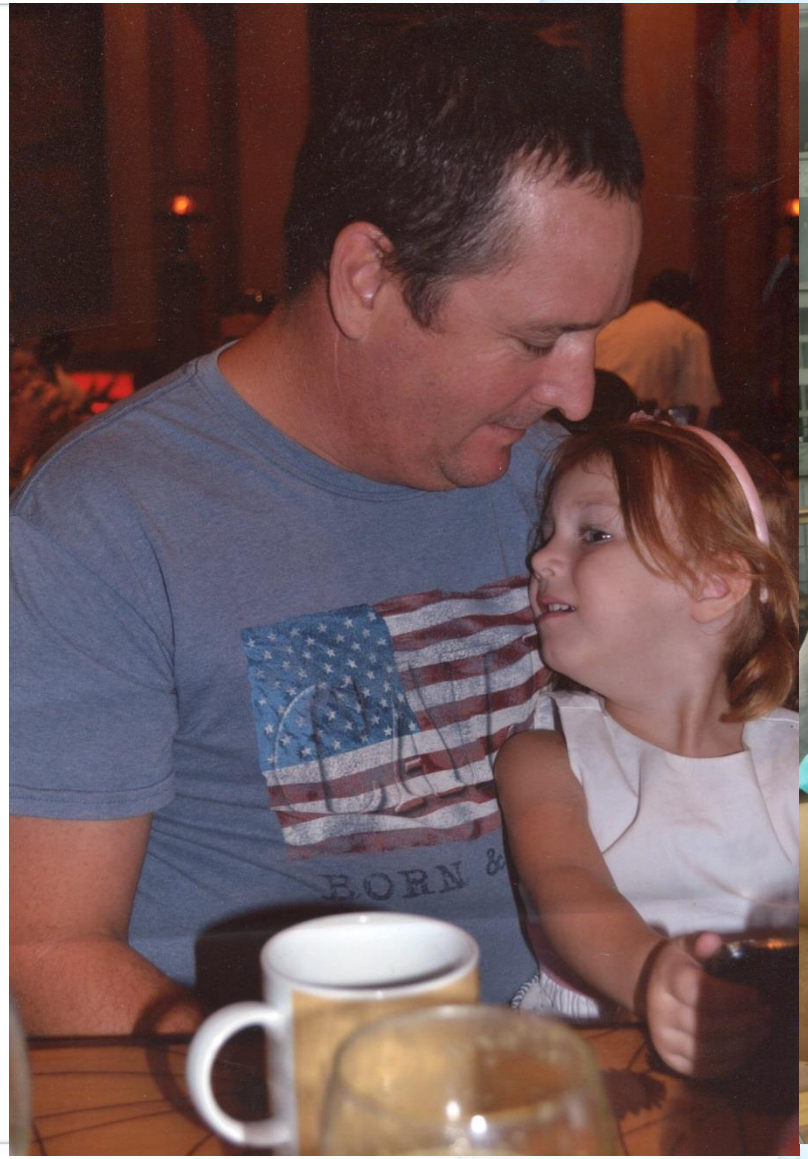
SCAP

Security Content Automation Protocol

OMB

Office of Management and Budget

My grandkids



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

History of the STIGS

IBM Server Proven

Business Partner IBM

History of the STIGS

DOD issues Directive 8500.1

Its purpose is to establish policy and assign responsibilities in order to achieve Department of Defense (DoD) information assurance (IA).

DISA created the STIGS in response to DoD 8500.1

The term STIGS was coined by DISA who creates configuration documents in support of the United States Department of Defense (DoD). The implementation guidelines include recommended administrative processes and span over the lifecycle of the device.

History of the STIGS

NIST Publishes Security Configuration Controls.

They do not include mainframe configuration controls.

NIST controls lead to the SCAP standard.

NIST Co-hosts with DHS a security configuration checklist at the NVD.

NIST 800-53 rev 3 included security controls in its catalog for both national security and non-national security systems.

History of the STIGS

DISA converts STIGS to SCAP format

DISA converts the STIGS to XCCDF format, the first step toward SCAP.

SP 800-126

NIST adopts STIGS

The NVD now contains checklist for the mainframe in the NCP.

OMB mandate

If NIST has a standard, all Federal agencies and all contractors processing data for a federal agency must conform to those standards.

History of the STIGS

- Version 4, Release 1.3, Feb. 2004
- Version 4, Release 1.4, Oct. 2004
- Version 4, Release 1.5, July 2005
- Version 5, Release 1.1, April 2006
- Version 5, Release 2.1, Nov. 2006
- Version 5, Release 2.2, March 2007
- Version 5, Release 2.3, May 2007
- Version 5, Release 2.6, Nov. 2007
- Version 5, Release 2.10, Dec. 2008

History of the STIGS

Version 5.2.10

The last release of the STIG Guideline (1000 page booklet that contained all the rationale behind the configuration control).

Version 6.1

This release and all subsequent released as SRR checklists only.

Version 6.2

XCCDF expressed checklist in line with Security Content Automation Protocol (SCAP). NIST 800-126

Version 6.24

Released on July 24, 2015 is the current release.

History of the STIGS

The *Control Correlation Identifier* (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise an IA control or IA best practice. CCI bridges the gap between high-level policy expressions and low-level technical implementations. CCI allows a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control. This ability to trace security requirements from their origin (e.g., regulations, IA frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple IA compliance frameworks. CCI also provides a means to objectively rollup and compare related compliance assessment results across disparate technologies..

Statistics

1	Addendum
6.22	is current version of DISA STIGS
30	separate DISA XML Documents
47	Different categories of checks
171	pages in Addendum
368	separate and distinct checks
1000s	of actual test

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Categories of STIG Checks

IBM Server Proven
Business Partner IBM

Categories of STIG Checks

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

- ✓ z/OS Data Analysis (AAMV)
- ✓ Security Server (RACF) Data Analysis (ACP, RACF
- ✓ CA-1 (Tape Management System) Data Analysis (ZCA1)
- ✓ CICS Data Analysis (ZCIC)
- ✓ CL/Supersession Data Analysis (ZCLS)
- ✓ DBMS Data Analysis (ZDBM)
- ✓ Front End Processor Data Analysis (ZFEP)
- ✓ IBM Communications Server Data Analysis (IFTP,ISLG,ITCP,ITNT,IUTN)
- ✓ Integrated Cryptographic Services Facility (ZICS)
- ✓ Integrated Database Management System (IDMS) Data Analysis (ZIDM)

Categories of STIG Checks

- ✓ BMC Control-D, Control–M, Control-O and IOA checks (ZCDT, ZCDM, ZCDO,ZIOA
- ✓ SDSF Data Analysis (ZISF)
- ✓ DFSMS Data Analysis (ZSMS)
- ✓ TSO Data Analysis (ZTSO)
- ✓ UNIX System Services Data Analysis (ZUSS)
- ✓ VTAM Data Analysis (ZVTM)
- ✓ WebSphere Application Server for z/OS Analysis (ZWAS)
- ✓ WebSphere MQSeries for z/OS Analysis (ZWMQ)
- ✓ Hardware Configuration Definition (ZHCD)
- ✓ Tivoli Asset Discovery (ZTAD)
- ✓ Catalog Solutions (ZCSL)
- ✓ Roscoe (ZROS)
- ✓ SRR Audit (ZSRR)

Categories of STIG Checks

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

- ✓ Tivoli Asset Discovery (ZTAD)
- ✓ Catalog Solutions (ZCSL)
- ✓ Roscoe (ZROS)
- ✓ SRR Audit (ZSRR)
- ✓ Transparent Data Migration Facility Data Analysis (ZTDM)
- ✓ NetView Data Analysis (ZNET)
- ✓ Vanguard Security Solutions (ZVSS)

Categories of STIG Checks

- ✓ CA Common Services (ZCCS)
- ✓ CA MIM (ZMIM)
- ✓ CA VTAPE (ZVTA)
- ✓ CA MICS (ZCMC)
- ✓ Compuware Abend-AID (ZAID)
- ✓ IBM CSSMTP (ZSMT)
- ✓ IBM Health Checker (ZHCK)
- ✓ IBM SDSF (SDSF)
- ✓ QWEST NC-PASS (ZNCP)
- ✓ CA MICS Resource Management (ZMIC)
- ✓ CA MIM Resource Sharing (ZMIM)
- ✓ BMC MAINVIEW (ZMVZ)

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Anatomy of a STIG Check

IBM Server Proven

Business Partner IBM

Anatomy of a STIG

Group ID (Vulid): V-6981
Group Title: ZUSS0036
Rule ID: SV-7284r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZUSS0036
Rule Title: z/OS UNIX MVS HFS directory(s) with "other" write permission bit set are not properly defined.

Vulnerability Discussion: For the z/OS UNIX environment, there are MVS data sets that contain operating system components, MVS data sets that contain HFS file systems with operating system components, and MVS data sets that contain HFS file systems with application system and user data. All of these MVS data sets require definitions in the ACP to enforce desired access controls. In addition, the UNIX permission bits must be properly set on the HFS directories and files to enforce desired access controls.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2, DCSL-1, ECCD-1, ECCD-2

Anatomy of a STIG

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection: - USSCMDS.RPT(OWDIR)

b) If there are no directories that have the other write permission bit set on without the sticky bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a “t” or “T” in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be “drwxrwxrwt”.

c) If all directories that have the other write permission bit set on do not contain any files with the setuid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an “s” or “S” in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be “-rwsrwxrwx”.

d) If all directories that have the other write permission bit set on do not contain any files with the setgid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an “s” or “S” in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be “-rwxrwsrwx”.

e) If (b), (c), or (d) above is untrue, this is a FINDING.

Anatomy of a STIG

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Fix Text: The systems programmer will verify the following:

a) There are no directories that have the other write permission bit set on without the sticky bit set on.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a “t” or “T” in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be “drwxrwxrwt”.

b) All directories that have the other write permission bit set on do not contain any files with the setuid bit set on.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an “s” or “S” in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be “-rwsrwxrwx”.

c) All directories that have the other write permission bit set on do not contain any files with the setgid bit set on.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an “s” or “S” in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be “-rwxrwsrwx”.

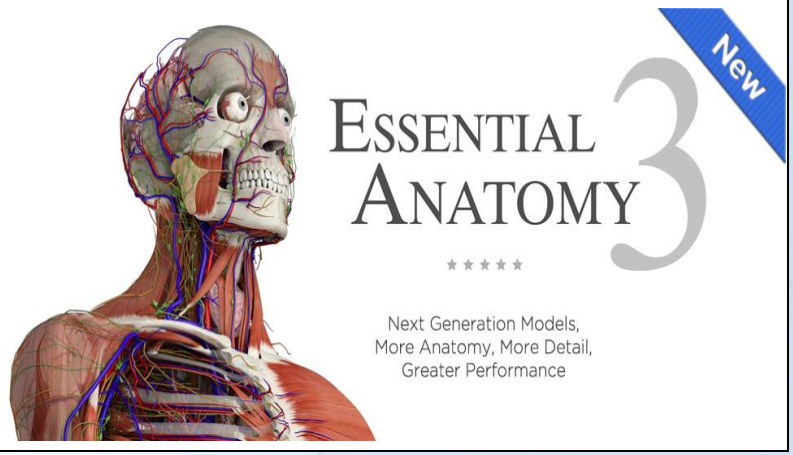
CCI: CCI-000213

CCI: CCI-002234

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Anatomy of a CCI

Control Correlation Identifier



IBM Server Proven
Business Partner IBM

Anatomy of a CCI

CCI:	CCI-000213	**Status:**	draft
Contributor:	DISA FSO	**Published Date:**	2009-09-14

Definition: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Type: technical

References: NIST: NIST SP 800-53 (v3): AC-3

NIST: NIST SP 800-53 Revision 4 (v4): AC-3

NIST: NIST SP 800-53A (v1): AC-3.1

Anatomy of a CCI

CCI:	CCI-002234	**Status:**	draft
Contributor:	DISA FSO	**Published Date:**	2013-06-24

Definition: The information system audits the execution of privileged functions.

Type: technical

References: NIST: NIST SP 800-53 Revision 4 (v4 : AC-6 (9)

Checks of Interest

Rule Version (STIG-ID): ACP00282

Rule Title: z/OS system commands are improperly protected.

Vulnerability Discussion: z/OS system commands provide a method of controlling the operating environment. Failure to properly control 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.

Checks:

The MVS.** resource is defined to the OPERCMDS class with a default access of NONE and all (i.e., failures and successes) access logged.

Access to z/OS system commands defined in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum, is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).
NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Stigs of Interest

IBM Server Proven

Business Partner IBM

Stigs of Interest

Group ID (Vulid): V-23837
Group Title: ACP00340
Rule ID: SV-28773r2_rule
Severity: CAT II
Rule Version (STIG-ID): ACP00340
Rule Title: z/OS Baseline reports are not reviewed and validated to ensure only authorized changes have been made within the z/OS operating system. This is a current DISA requirement for change management to system libraries.

Vulnerability Discussion: A product that generates reports validating changes, additions or removal from APF and LPA libraries, as well as changes to SYS1.PARMLIB PDS members, should be run against system libraries to provide a baseline analysis to allow monitoring of changes to these libraries. Failure to monitor and review these reports on a regular bases and validating any changes could threaten the integrity and availability of the operating system environment, and compromise the confidentiality of customer data.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, DCPR-1, DCSL-1, ECAT-1, ECAT-2

Stigs of Interest

Check Content:

Note: For DISA sites the product used to generate these reports is CA-Auditor.

z/OS Baseline Reporting – Review period is based upon 10% random selection of z/OS Domains at the given site by the IAO. Such schedule shall not be published or known – selection of z/OS domains shall be randomly selected each week.

a) The z/OS Baseline reports (as indentified by report/function CS212C (Updates to SYS1.PARMLIB), CS221C (APF library statistics) and CS243C (LPA library statistics) shall be reviewed and validated with the appropriate system programming staff on a weekly schedule, or as required based on INFOCON Level requirements.

Note: Sites that do not utilize CA-Auditor, review the z/OS STIG Addendum for the samples of the CA-Auditor report to identify the information to collect. The INFOCON Level requirements can be found in STRATEGIC COMMAND DIRECTIVE (SD) 527-1.

Stigs of Interest

b) Such reports shall be compared with known and authorized changes to the specific z/OS domain. Any anomalies found shall be documented as a potential incident and must be investigated with written documentation as proof showing such review was completed.

c) If the baseline reports are being reviewed and samples of the baseline reports exist, there is NO FINDING.

d) If the baseline reports are not being reviewed or samples of the reports do not exist this is a FINDING.

Stigs of Interest

Fix Text: Validate the results of the z/OS Baseline reports with the appropriate system programming staff.

For sites that have CA-Auditor, minimally the following functional reports shall be validated: CS212C, CS221C and CS243C..

Compliance of this would be for the appropriate system programming staff to review the specific baseline reports and to affirm the changes are legitimate. Any identified exception or anomaly shall be reported, researched and documented. Such documentation shall be made available for auditor reviews.

The baseline reports should be created as GDGs, and should be saved for at least a year. Please see the z/OS Addendum under ACP00340 for additional instructions, and a sample of the CA-Auditor reports that should be run for that utilizes CA-Auditor.

CCI: CCI-000294
CCI: CCI-000295
CCI: CCI-000296
CCI: CCI-001819
CCI: CCI-001823
CCI: CCI-002087

Stigs of Interest

Group ID (Vulid): V-7482
Group Title: ACP00282
Rule ID: SV-7919r1_rule
Severity: CAT II
Rule Version (STIG-ID): ACP00282
Rule Title: z/OS system commands are improperly protected.

Vulnerability Discussion: z/OS system commands provide a method of controlling the operating environment. Failure to properly control 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.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Stigs of Interest

Group ID (Vulid): V-7482
Group Title: ACP00282
Rule ID: SV-7919r1_rule
Severity: CAT II
Rule Version (STIG-ID): ACP00282
Rule Title: z/OS system commands are improperly protected.

Vulnerability Discussion: z/OS system commands provide a method of controlling the operating environment. Failure to properly control 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.

Responsibility: Information Assurance Officer
IAControls: DCCS-1, DCCS-2, ECAR-1, ECAR-2, ECCD-1, ECCD-2

Stigs of Interest

Check Content:

a) Refer to the following report produced by the Data Set and Resource Data Collection:

- SENSITVE.RPT(OPERCMDS)

Automated Analysis
Refer to the following report produced by the Data Set and Resource Data Collection:

- PDI(ACP00282)

b) The MVS.** resource is defined to the OPERCMDS class with a default access of NONE and all (i.e., failures and successes) access logged.

c) Access to z/OS system commands defined in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum, is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

Stigs of Interest

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

d) All access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled Required Controls on z/OS System Commands, in the z/OS STIG Addendum.

e) If either (b), (c), or (d) above is untrue for any z/OS system command resource, this is a FINDING.

f) If (b), (c), and (d) above are true, there is NO FINDING.

Stigs of Interest

Fix Text: z/OS system commands provide control over z/OS functions and can compromise security if misused. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the z/OS system commands that can be entered by particular operators.

Some commands are particularly dangerous and should only be used when all less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL.

Apply the following recommendations when implementing security:

1) The MVS.** resource is defined to the OPERCMDS class with a default access of NONE and all (i.e., failures and successes) access logged.

2) Access to z/OS system commands defined in the "Required Controls on z/OS System Commands" table in the zOS STIG Addendum is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users).

Stigs of Interest

NOTE: Use the GROUP category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

3) All access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled "Required Controls on z/OS System Commands" in the zOS STIG Addendum.

Stigs of Interest

A sample set of commands to define and permit access to system command resources is shown here:

RDEF OPERCMDS MVS.** UACC(NONE) OWNER(<syspaudt>)
AUDIT(ALL(READ)) DATA("set up deny-by-default profile per srr pdi acp00282')

Then, in accordance with the referenced table, use the following template to define profiles for each command:

RDEF OPERCMDS <systemcommandprofile> UACC(NONE)
OWNER(<syspaudt>) AUDIT(ALL(READ))

PERMIT <systemcommandprofile> CLASS(OPERCMDS) ID(<groupname>)
ACCESS(<accesslevel>)

CCI: CCI-000213
CCI: CCI-002234
CCI: CCI-002235

Stigs of Interest

ACP00282 List of Commands to Check

Stigs of Interest

Group ID (Vulid): V-6963
Group Title: ZUSS0016
Rule ID: SV-7264r1_rule
Severity: CAT II
Rule Version (STIG-ID): ZUSS0016
Rule Title: z/OS UNIX security parameters in /etc/rc not properly specified.

Vulnerability Discussion: Parameter settings in PARMLIB and /etc specify values for z/OS UNIX security controls. 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.

Responsibility: Systems Programmer
IAControls: DCCS-1, DCCS-2

Stigs of Interest

Check Content:

a) Refer to the following report produced by the UNIX System Services Data Collection:

- USSCMDS.RPT(ERC)

b) If all of the CHMOD commands in /etc/rc do not result in less restrictive access than what is specified in the SYSTEM DIRECTORY SECURITY SETTINGS Table and the SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum, there is NO FINDING.

NOTE: The use of CHMOD commands in /etc/rc is required in most environments to comply with the required settings, especially for dynamic objects such as the /dev directory.

Stigs of Interest

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)

c) If all of the CHAUDIT commands in /etc/rc do not result in less auditing than what is specified in the SYSTEM DIRECTORY SECURITY SETTINGS Table and the SYSTEM FILE SECURITY SETTINGS Table in the z/OS STIG Addendum, there is NO FINDING.

NOTE: The use of CHAUDIT commands in /etc/rc may not be necessary. If none are found, there is NO FINDING.

Stigs of Interest

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
- no auditing

d) If the _BPX_JOBNAME variable is appropriately set (i.e., to match daemon name) as each daemon (e.g., syslogd, inetd) is started in /etc/rc, there is NO FINDING.

NOTE: If _BPX_JOBNAME is not specified, the started address space will be named using an inherited value. This could result in reduced security in terms of operator command access.

e) If (b), (c), or (d) above is untrue, this is a FINDING

Stigs of Interest

Fix Text: Review the settings in the /etc/rc. The /etc/rcfile is the system initialization shell script. When z/OS UNIX kernel services start, /etc/rc is executed to set file permissions and ownership for dynamic system files and to perform other system startup functions such as starting daemons. There can be many commands in /etc/rc. There are two specific guidelines that must be followed:
Verify that The CHMOD or CHAUDIT command does not result in less restrictive security than than what is specified in the table in the z/OS STIG addendum under the SYSTEM DIRECTORY SECURITY SETTINGS,

Immediately prior to each command that starts a daemon, the _BPX_JOBNAME variable must be set to match the daemon's name (e.g., inetd, syslogd). The use of _BPX_USERID is at the site's discretion, but is recommended.

CCI: CCI-000366
CCI: CCI-001499
CCI: CCI-002234

Stigs of Interest

Table 8 - System Directory Security Settings

Note: Any Directory that uses AUTOMOUNT, does not require the specified settings.

Referenced by: ZUSS0016, ZUSS0034

SYSTEM DIRECTORY SECURITY SETTINGS			
DIRECTORY	*PERMISSION BITS*	*USER AUDIT BITS*	*FUNCTION*
/ [root]	755	faf	Root level of all file systems. Holds critical mount points.
/bin	1755	fff	Shell scripts and executables for basic functions
/dev	1755	fff	Character-special files used when logging into the OMVS shell and during C language program compilation. Files are created during system IPL and on a per-demand basis.
/etc	1755	faf	Configuration programs and files (usually with locally customized data) used by z/OS UNIX and other product initialization processes
/lib	1755	fff	System libraries including dynamic link libraries and files for static linking
/samples	1755	fff	Sample configuration and other files
/tmp	1777	fff	Temporary data used by daemons, servers, and users. *NOTE*: /tmp must have the sticky bit on to restrict file renames and deletions.
/u	1755	fff	Mount point for user home directories and optionally for third-party software and other local site files
/usr	1755	fff	Shell scripts, executables, help (man) files and other data. Contains sub-directories (e.g., lpp) and mount points used by program products that may be in separate file systems.
/var	1775	fff	Dynamic data used internally by products and by elements and features of z/OS UNIX.

NOTE: The sticky bit is set on to restrict file renames and file deletions or subdirectory deletions.

Stigs of Interest

Table 9 - System File Security Settings

Referenced by: ZUSS0035, ZUSS0016

SYSTEM FILE SECURITY SETTINGS			
FILE	*PERMISSION BITS*	*USER AUDIT BITS*	*FUNCTION*
/bin/sh	1755	faf	z/OS UNIX shell ***NOTE***: /bin/sh has the sticky bit on to improve performance.
/dev/console	740	fff	The system console file receives messages that may require System Administrator (SA) attention.
/dev/null	666	fff	A null file; data written to it is discarded.
/etc/auto.master and any *mapname* files	740	faf	Configuration files for automount facility
/etc/inetd.conf	740	faf	Configuration file for network services
/etc/init.options	740	faf	Kernel initialization options file for z/OS UNIX environment
/etc/log	744	fff	Kernel initialization output file
/etc/profile	755	faf	Environment setup script executed for each user
/etc/rc	744	faf	Kernel initialization script for z/OS UNIX environment
/etc/steplib	740	faf	List of MVS data sets valid for set-user-ID and set-group-ID executables
/etc/tablename	740	faf	List of z/OS userids and group names with corresponding alias names
/usr/lib/cron/at.allow /usr/lib/cron/at.deny	700	faf	Configuration files for the at and batch commands
/usr/lib/cron/cron.allow /usr/lib/cron/cron.deny	700	faf	Configuration files for the crontab command

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Changes Since 6.20

IBM Server Proven
Business Partner IBM

Changes in 6.20

AAMV0380	Adding and removing SMF record types, AAMV0380. added types 41, 42, 102, 119 and 199.
ACP00120	Allowed access levels have changed. Read STIG for details.
ACP00270	Add BMC Mainview users IDs.
ACP00282	Added VARY TCPIP cmd.
RACF0580	Changes concerning FTP server userids.
RACF0680	The STIG was reworded, but I do not believe the wording affects the check.
ZCTM0020	Modified access levels for resource name $$CTMSTC.

Changes in 6.21

ZNET0040 – CNMSTYLE in DSIPARM DD statement changed to CxxSTYLE.

SECOPTS.OPERSEC=SAFPW configuration parameter has been removed.

ZCIC0020

Added Table 33a to Addendum, Section 11.5 CICS Requirements.

- Changes to Table 34b
- Added transaction CDBN
- Added transaction CEBT
- Added transaction CEPS
- Added transaction CHLP
- Added transaction CJSA

ZCICR021 (We call it ZCICX021)

- Table 40 in Addendum, APPDAUDT added to resources FILE, PROGRAM, TRANSACTION

Changes in 6.22

Added CCIs to checks

Changes in 6.23

ZCTR0002 Modified access requirements for AUTOAUDT and PCSPAUDT to WRITE and/or greater.

ZISF0020 Modified GROUP.group-name checks to specify only one entry stating that additional analysis will be required to justify access.

ZISF0040 Added requirement for AUPDT=0

ZCLS0042 Corrected exit specified for CAC logon process

Updated AAMV0450 with current references.

Changes in 6.23

Updated ACP00120 with requirement to protect new RACF Exit SPECLIST(character list) and change example to specify SPECLIST(character list)

Updated RACF0460 with new Password guidance.

New Vulnerability RACF0462 with extended Password guidance.

Changes in 6.23

Addendum changes

Modified z/OS Addendum to add resources to Table 55 – BMC MAINVIEW Resources

Modified z/OS Addendum to change access requirements to resources to Table 15 - Controls on z/OS System Commands

Added new table to Addendum for RACF Password exit.

Changes in 6.24

ZCTOR001

Updated to allow OPERAUDT READ access for the BMC CONTROL-O STC Datasets.

Deleted the IDMS checks

ZJES0032

Updated to specify The RACF resources and/or generic equivalent in the WRITER class are defined with a default access of NONE. The RACF resource access authorizations are defined with UACC(NONE) and NOWARNING.

ZMIMR020

Update to allow AUTOAUDT UPDATE access to resource MIMGR.FREE as shown in the STIG Addendum.

Added ZWMQ0014 back in. I was deleted

ANY Questions?

Thank You

Call us at 800-794-0014
or
email us at info@go2vanguard.com