

JANUARY 2021 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Apache Server 2.4 UNIX Server STIG, Version 2, Release 2

AS24-U1-000270

AS24-U1-000270 - Added clarity to the intent of the requirement.

AS24-U1-000930

AS24-U1-000930 - Added clarity regarding version requirement for proprietary compiles of Apache.

AS24-U1-000680

AS24-U1-000680 - Added additional steps in locating PidFile runtime directive.

AS24-U1-000250

AS24-U1-000250 - Check and fix content more appropriate for AS24-U1-000270.

Apache Server 2.4 UNIX Site STIG, Version 2, Release 1

AS24-U2-000390

AS24-U2-000390 - Corrected requirement to validate SSLCertificateKeyFile directive rather than SSLCertificateFile directive.

Apache Tomcat Application Sever 9 STIG, Version 2, Release 2

TCAT-AS-000090

TCAT-AS-000090 - Clarified Vulnerability Discussion and Check verbiage. Deleted the "not a finding" statement in the check to ensure the readonly setting is created.

TCAT-AS-000970

TCAT-AS-000970 - Consolidated with TCAT-AS-001300 and TCAT-AS-000810.

Apple OS X 10.13 STIG, Version 2, Release 1

AOSX-13-000054

AOSX-13-000054 - Added a requirement to configure ssh ciphers.

AOSX-13-000055

AOSX-13-000055 - Added a requirement to configure ssh macs

AOSX-13-000056

AOSX-13-000056 - Added a requirement to configure ssh key exchange algorithms.

Apple OS X 10.14 STIG, Version 2, Release 2

AOSX-14-000054

AOSX-14-000054 - Added a requirement to configure ssh ciphers.

AOSX-14-000055

AOSX-14-000055 - Added a requirement to configure ssh macs.

AOSX-14-000056

AOSX-14-000056 - Added a requirement to configure ssh key exchange algorithms.

AOSX-14-002069

AOSX-14-002069 - Updated the parent SRG requirement assigned to this rule. Updated the rule title to reflect the updated parent SRG requirement.

Apple OS X 10.15 STIG, Version 1, Release 3**AOSX-15-000054**

AOSX-15-000054 - Added a requirement to configure ssh ciphers.

AOSX-15-000055

AOSX-15-000055 - Added a requirement to configure ssh macs.

AOSX-15-000056

AOSX-15-000056 - Added a requirement to configure ssh key exchange algorithms.

AOSX-15-002009

AOSX-15-002009 - Updated the check command to use the correct configuration setting.

AOSX-15-002069

AOSX-15-002069 - Updated the parent SRG requirement assigned to this rule. Updated the rule title to reflect the updated parent SRG requirement.

AOSX-15-002005

AOSX-15-002005 - Corrected a spelling error in the check command.

Apple OS/iPad OS 13 STIG, Version 2, Release 1**AIOS-13-999999**

AIOS-13-999999 - Added new requirement to sunset STIG.

BIND 9.x STIG, Version 2, Release 1**BIND-9X-001060**

BIND-9X-001060 - Modified requirement fix to verify dnssec-enable is set to yes also. Added verbiage regarding dnssec-validation set to auto.

BlackBerry UEM STIG, Version 2, Release 1**BUEM-00-000630**

BUEM-00-000630 - Updated Check and Fix procedures.

BUEM-00-000010

BUEM-00-000010 - Updated Check and Fix procedures.

Canonical Ubuntu 16.04 LTS STIG Benchmark, Version 2, Release 2**UBTU-16-030230**

Updated oval:mil.disa.stig.ubuntu1604:ste:23300 to remove the dash after "aes" in the quoted part of the regular expression.

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

UBTU-16-030400

Changed OVAL to check that X11Forwarding is set to "no" to maintain alignment with the STIG.

Canonical Ubuntu 16.04 LTS STIG, Version 2, Release 2

UBTU-16-020350

UBTU-16-020350 - Added missing "euid" and "egid" definitions as needed.

UBTU-16-030230

UBTU-16-030230 - Updated cipher order from strongest to weakest in the requirement.

UBTU-16-030400

UBTU-16-030400 - Updated the method in which the rule handles ssh-based X11 forwarding.

UBTU-16-030401

UBTU-16-030401 - Added requirement to prevent remote hosts from connecting to the proxy display.

UBTU-16-020460

UBTU-16-020460 - Corrected a typo in the fix text.

UBTU-16-020560

UBTU-16-020560 - Added a line to the fix to address 32-bit architecture.

UBTU-16-020570

UBTU-16-020570 - Added a line to the fix to address 32-bit architecture.

UBTU-16-020651

UBTU-16-020651 - Removed duplicate requirement.

UBTU-16-020700

UBTU-16-020700 - Removed an unnecessary 32-bit architecture reference from the audit rule.

UBTU-16-030240

UBTU-16-030240 - Updated MACs order from strongest to weakest in the requirement.

Canonical Ubuntu 18.04 LTS STIG, Version 2, Release 2

UBTU-18-010358

UBTU-18-010358 - Added missing "euid" and "egid" definitions as needed.

UBTU-18-010501

UBTU-18-010501 - Updated the fix text to reference /etc/chrony/chrony.conf.

UBTU-18-010021

UBTU-18-010021 - Update the package name and daemon names to "mfetp". Updated the command to check the running status of the daemon.

UBTU-18-010411

UBTU-18-010411 - Updated cipher order from strongest to weakest in the requirement.

UBTU-18-010418

UBTU-18-010418 - Added requirement to handle ssh-based X11 forwarding.

UBTU-18-010419

UBTU-18-010419 - Added requirement to prevent remote hosts from connecting to the proxy display.

UBTU-18-010417

UBTU-18-010417 - Updated MACs order from strongest to weakest in the requirement. Updated the severity to a CAT II.

Canonical Ubuntu 18.04 STIG Benchmark, Version 2, Release 1

NA

Rebundled to capture the changes to the STIG including updated rule IDs.

UBTU-18-010411

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

Cisco NX-OS Switch NDM STIG, Version 2, Release 1

CISC-ND-000290

CISC-ND-000290 - Added line to fix text for adding 'log' to deny ACL's.

Database SRG, Version 3, Release 1

SRG-APP-000456-DB-000400

SRG-APP-000456-DB-000400 - Added new requirement added to ensure DBMS product is supported by the vendor.

SRG-APP-000360-DB-000320

SRG-APP-000360-DB-000320 - Corrected check text.

Firewall SRG, Version 2, Release 1

SRG-NET-000098-FW-000021

SRG-NET-000098-FW-000021 - Corrected CCI.

Google Chrome for Windows STIG Benchmark, Version 2, Release 2

NA

Rebundled to capture the changes to the STIG including updated rule IDs.

Google Chrome STIG, Version 2, Release 2

DTBC-0006

DTBC-0006 - Updated registry value.

HBSS ePO 5.x STIG, Version 2, Release 2

H30243

H30243 - Correct Agent wake-up communication port back to 591 per HBSS PMO.

H30700

H30700 - Removed references to Policy Auditor as a viable FIM.

H20200 - N

H20200 - Modified criteria to specify Syslog instead of Arcsight.

H36960

H36960 - Added requirement for a firewall rule for outbound to Syslog.

H37560

H37560 - Requirement reworded for specifics relating to server settings for Syslog configuration.

H30140

H30140 - Updated to reflect correction OPORD.

H37520

H37520 - Updated with references to ACCM EOL and transition to PA.

H37580

H37580 - Removed references to Build 2 servers.

IBM zOS RACF STIG, Version 8, Release 2

RACF-CE-000020

RACF-CE-000020 - Corrected typo in command.

RACF-US-000190

RACF-US-000190 - Changed to more efficient display command in Check.

Infoblox 7.x DNS STIG, Version 2, Release 1

IDNS-7X-000710

IDNS-7X-000710 - Modified finding statement to be in sync with requirement.

JBoss EAP 6.3 STIG, Version 2, Release 1

JBOS-AS-000015

JBOS-AS-000015 - Updated Vulnerability Discussion and Fix to account for TLSV1.2.

JBOS-AS-000650

JBOS-AS-000650 - Updated Vulnerability Discussion and Fix to account for TLSV1.2.

JBOS-AS-000655

JBOS-AS-000655 - Updated Vulnerability Discussion to account for TLSV1.2.

Juniper Router RTR STIG, Version 2, Release 1

JUNI-RT-000235

JUNI-RT-000235 - Added requirement to prohibit use of IPv6 Site Local addresses.

JUNI-RT-000381

JUNI-RT-000381 - Added requirement to suppress IPv6 Router Advertisements at external interfaces.

JUNI-RT-000382

JUNI-RT-000382 - Added requirement to drop IPv6 packets with a Routing Header type 0, 1, or 3-255.

JUNI-RT-000383

JUNI-RT-000383 - Added requirement to drop IPv6 packets containing a Hop-by-Hop header with invalid option type values.

JUNI-RT-000384

JUNI-RT-000384 - Added requirement to drop IPv6 packets containing a Destination Option header with invalid option type values.

JUNI-RT-000385

JUNI-RT-000385 - Added requirement to drop IPv6 packets containing an extension header with the Endpoint Identification option.

JUNI-RT-000386

JUNI-RT-000386 - Added requirement to drop IPv6 packets containing the NSAP address option within Destination Option header.

JUNI-RT-000387

JUNI-RT-000387 - Added requirement to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type.

Microsoft DotNet Framework 4.0 STIG Benchmark, Version 2, Release 1

NA

Rebundled to capture the changes to the STIG including updated rule IDs.

Microsoft DotNet Framework 4.0 STIG, Version 2, Release 1

APPNET0075

APPNET0075 - Updated check and fix to include the 32-bit key with 64-bit systems.

Microsoft Exchange 2013 Mailbox Server STIG, Version 2, Release 1

EX13-MB-000115

EX13-MB-000115 - Modified Rule Title, Check, and Fix to be for internal receive connectors instead of send connectors.

Microsoft Exchange 2016 Edge Transport Server STIG, Version 2, Release 2

EX16-ED-000570

EX16-ED-000570 - Modified Rule Title and intent of requirement to specify hyperlink should be rendered unclickable rather than removed.

Microsoft Exchange 2016 Mailbox Server STIG, Version 2, Release 2**EX16-MB-000030**

EX16-MB-000030 - Added note to specify requirement is not applicable to Exchange on classified or completely closed networks.

Microsoft SharePoint 2013 STIG, Version 2, Release 1**SP13-00-000210**

SP13-00-000210 - Altered permissions.

Microsoft SQL Server 2016 Instance STIG, Version 2, Release 2**SQL6-D0-008400**

SQL6-D0-008400 - Changed PKI private keys stored requirement to a CAT 1.

SQL6-D0-011800

SQL6-D0-011800 - Removed duplicate 'DATABASE_OWNERSHIP_CHANGE_GROUP' from SQL.

Mozilla Firefox STIG Configuration Files, Version 5, Release 1**NA**

Removed metadata pointing to DPMS 2.x Rule IDs

Mozilla Firefox STIG for RHEL Benchmark, Version 5, Release 1**DTBF230**

Removed requirement from automated benchmark.

DTBF030

Updated OVAL to look in more locations for configuration data.

DTBF050

Updated OVAL to look in more locations for configuration data.

DTBF085

Updated OVAL to look in more locations for configuration data.

DTBF090

Updated OVAL to look in more locations for configuration data.

DTBF105

Updated OVAL to look in more locations for configuration data.

DTBF110

Updated OVAL to look in more locations for configuration data.

DTBF140

Updated OVAL to look in more locations for configuration data.

DTBF150

Updated OVAL to look in more locations for configuration data.

DTBF160

Updated OVAL to look in more locations for configuration data.

DTBF180

Updated OVAL to look in more locations for configuration data.

DTBF181

Updated OVAL to look in more locations for configuration data.

DTBF182

Updated OVAL to look in more locations for configuration data.

DTBF183

Updated OVAL to look in more locations for configuration data.

DTBF186

Updated OVAL to look in more locations for configuration data.

DTBF190

Updated OVAL to look in more locations for configuration data.

DTBF195

Updated OVAL to look in more locations for configuration data.

DTBF200

Updated OVAL to look in more locations for configuration data.

DTBF205

Updated OVAL to look in more locations for configuration data.

DTBF210

Updated OVAL to look in more locations for configuration data.

DTBF215

Updated OVAL to look in more locations for configuration data.

DTBF220

Updated OVAL to look in more locations for configuration data.

DTBF225

Updated OVAL to look in more locations for configuration data.

DTBF235

Updated OVAL to look in more locations for configuration data.

Mozilla Firefox STIG for Windows Benchmark, Version 5, Release 1**DTBF230**

Removed requirement from automated benchmark.

DTBF030

Updated OVAL to look in more locations for configuration data.

DTBF050

Updated OVAL to look in more locations for configuration data.

DTBF085

Updated OVAL to look in more locations for configuration data.

DTBF090

Updated OVAL to look in more locations for configuration data.

DTBF105

Updated OVAL to look in more locations for configuration data.

DTBF110

Updated OVAL to look in more locations for configuration data.

DTBF140

Updated OVAL to look in more locations for configuration data.

DTBF150

Updated OVAL to look in more locations for configuration data.

DTBF160

Updated OVAL to look in more locations for configuration data.

DTBF180

Updated OVAL to look in more locations for configuration data.

DTBF181

Updated OVAL to look in more locations for configuration data.

DTBF182

Updated OVAL to look in more locations for configuration data.

DTBF183

Updated OVAL to look in more locations for configuration data.

DTBF186

Updated OVAL to look in more locations for configuration data.

DTBF190

Updated OVAL to look in more locations for configuration data.

DTBF195

Updated OVAL to look in more locations for configuration data.

DTBF200

Updated OVAL to look in more locations for configuration data.

DTBF205

Updated OVAL to look in more locations for configuration data.

DTBF210

Updated OVAL to look in more locations for configuration data.

DTBF215

Updated OVAL to look in more locations for configuration data.

DTBF220

Updated OVAL to look in more locations for configuration data.

DTBF225

Updated OVAL to look in more locations for configuration data.

DTBF235

Updated OVAL to look in more locations for configuration data.

Mozilla Firefox STIG, Version 5, Release 1

NA

Added FireFox_Linux_README.txt to bundle.

DTBF230

DTBF230 - Removed deprecated requirement.

Oracle JRE 8 Windows STIG, Version 2, Release 1

JRE8-WN-000180

JRE8-WN-000180 - Modified to state supported version.

Oracle Linux 5 STIG, Version 2, Release 2

NA

The Oracle Linux 5 STIG dropped from Vendor support in November 2020. This STIG was placed on the Sunset list due to lack of vendor support.

GEN005505

GEN005505 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

Oracle Linux 6 STIG, Version 2, Release 2

OL6-00-000228

OL6-00-000228 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

OL6-00-000230

OL6-00-000230 - Updated timeout interval to ten minutes.

OL6-00-000243

OL6-00-000243 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

Oracle Linux 7 STIG Benchmark, Version 2, Release 2

OL07-00-020620

Updated OVAL to handle more than one interactive user in /etc/passwd.

OL07-00-021350

Added logic to OVAL to check for the existence of the /etc/system-fips file

OL07-00-040110

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

OL07-00-040400

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

OL07-00-040710

Changed OVAL to check that X11Forwarding is set to "no" to maintain alignment with the STIG.
Update the OVAL to check that X11Forwarding is disabled.

Oracle Linux 7 STIG, Version 2, Release 2

OL07-00-010320

OL07-00-010320 - Updated Fix Text to remove inaccurate information.

OL07-00-020620

OL07-00-020620 - Updated Check Content command.

OL07-00-020690

OL07-00-020690 - Updated Check Content command.

OL07-00-020700

OL07-00-020700 - Updated Check Content command.

OL07-00-040110

OL07-00-040110 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

OL07-00-040400

OL07-00-040400 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

OL07-00-020630

OL07-00-020630 - Updated Check Content command.

OL07-00-020640

OL07-00-020640 - Updated Check Content command.

OL07-00-020650

OL07-00-020650 - Updated Check Content command.

OL07-00-021000

OL07-00-021000 - Updated Check Content command.

OL07-00-021310

OL07-00-021310 - Updated Check Content command.

OL07-00-040480

OL07-00-040480 - Removed this requirement as DNSSEC is better handled thru a DNS-centric STIG. (e.g., BIND STIG)

OL07-00-040710

OL07-00-040710 - Updated Rule Title, Vulnerability Discussion, Check Content, Fix Content to disable X11Forwarding and downgraded requirement to a CAT II.

OL07-00-040711

OL07-00-040711 - Added requirement to bind the X11 forwarding server to the loopback address.

Red Hat Enterprise Linux 6 STIG Benchmark, Version 2, Release 2

RHEL-06-000230

Update the OVAL to check the ClientAliveInterval is set to 600 seconds or less.

Red Hat Enterprise Linux 6 STIG, Version 2, Release 2

NA

The Red Hat Enterprise Linux 6 STIG dropped from Vendor support in November 2020. This STIG was placed on the Sunset list due to lack of vendor support.

RHEL-06-000228

RHEL-06-000228 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

RHEL-06-000230

RHEL-06-000230 - Updated timeout interval to ten minutes.

RHEL-06-000243

RHEL-06-000243 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

RHEL-06-000244

RHEL-06-000244 - Combined this requirement with RHEL-06-000228.

Red Hat Enterprise Linux 7 STIG Benchmark, Version 3, Release 2

RHEL-07-021350

Added logic to OVAL to check for the existence of the `/etc/system-fips` file

RHEL-07-020620

Updated OVAL to handle more than one interactive user in `/etc/passwd`.

RHEL-07-040110

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

RHEL-07-040400

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

RHEL-07-040710

Changed OVAL to check that X11Forwarding is set to "no" to maintain alignment with the STIG.
Update the OVAL to check that X11Forwarding is disabled.

Red Hat Enterprise Linux 7 STIG, Version 3, Release 2

RHEL-07-010320

RHEL-07-010320 - Updated Fix Text to remove inaccurate information.

RHEL-07-020620

RHEL-07-020620 - Updated Check Content command.

RHEL-07-020630

RHEL-07-020630 - Updated the command in the Check Content.

RHEL-07-020640

RHEL-07-020640 - Updated Check Content command.

RHEL-07-020650

RHEL-07-020650 - Updated Check Content command.

RHEL-07-020690

RHEL-07-020690 - Updated Check Content command.

RHEL-07-020700

RHEL-07-020700 - Updated Check Content command.

RHEL-07-021000

RHEL-07-021000 - Updated Check Content command.

RHEL-07-021310

RHEL-07-021310 - Updated Check Content command.

RHEL-07-040110

RHEL-07-040110 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

RHEL-07-040400

RHEL-07-040400 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

RHEL-07-040710

RHEL-07-040710 - Updated Rule Title, Vulnerability Discussion, Check Content, Fix Content to disable X11Forwarding and downgraded requirement to a CAT II.

RHEL-07-040711

RHEL-07-040711 - Added requirement to bind the X11 forwarding server to the loopback address.

Router SRG, Version 4, Release 1**SRG-NET-000230-RTR-000001**

SRG-NET-000230-RTR-000001 - Provided clarification in the Vulnerability Discussion.

SLES 12 STIG Benchmark, Version 2, Release 2**SLES-12-020250**

Added OVAL content for the requirement.

SLES-12-020260

Added OVAL content for the requirement.

SLES-12-020280

Added OVAL content for the requirement.

SLES-12-020310

Added OVAL content for the requirement.

SLES-12-020320

Added OVAL content for the requirement.

SLES-12-020550

Added OVAL content for the requirement.

SLES-12-020560

Added OVAL content for the requirement.

SLES-12-020570

Added OVAL content for the requirement.

SLES-12-020580

Added OVAL content for the requirement.

SLES-12-020600

Added OVAL content for the requirement.

SLES-12-020610

Added OVAL content for the requirement.

SLES-12-020620

Added OVAL content for the requirement.

SLES-12-020630

Added OVAL content for the requirement.

SLES-12-020640

Added OVAL content for the requirement.

SLES-12-020670

Added OVAL content for the requirement.

SLES-12-020680

Added OVAL content for the requirement.

SLES-12-020690

Added OVAL content for the requirement.

SLES-12-020700

Added OVAL content for the requirement.

SLES-12-020710

Added OVAL content for the requirement.

SLES-12-020720

Added OVAL content for the requirement.

SLES-12-030170

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

SLES-12-030180

Update the OVAL to check for the updated cipher order from strongest to weakest in the requirement.

SLES-12-030260

Changed OVAL to check that X11Forwarding is set to "no" to maintain alignment with the STIG.

SLES-12-010400

Corrected OVAL IDs to include "sles12" rather than "rhel7"

SLES-12-010410

Corrected OVAL IDs to include "sles12" rather than "rhel7"

Solaris 10 SPARC STIG Benchmark, Version 2, Release 2

GEN005500

Updated the OVAL to return unknown if sshd_config is not in the expected location.

Solaris 10 SPARC STIG, Version 2, Release 2

GEN005505

GEN005505 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

GEN005201

GEN005201 - Added requirement to disable X11 forwarding.

GEN005202

GEN005202 - Added requirement to bind the X11 forwarding server to the loopback address.

Solaris 10 X86 STIG Benchmark, Version 2, Release 2

GEN005500

Updated the OVAL to return unknown if sshd_config is not in the expected location.

Solaris 10 x86 STIG, Version 2, Release 2

GEN005505

GEN005505 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

GEN005201

GEN005201 - Added requirement to disable X11 forwarding.

GEN005202

GEN005202 - Added requirement bind the X11 forwarding server to the loopback address.

Solaris 11 SPARC STIG Benchmark, Version 2, Release 2

NA

Rebundled to capture the changes to the STIG including updated rule IDs.

Solaris 11 SPARC STIG, Version 2, Release 2

SOL-11.1-020540

SOL-11.1-020540 - Updated Check Content to remove unnecessary verbiage.

SOL-11.1-040010

SOL-11.1-040010 - Updated requirement to incorporate an increased granularity in password management.

SOL-11.1-040030

SOL-11.1-040030 - Updated requirement to incorporate an increased granularity in password management.

SOL-11.1-040331

SOL-11.1-040331 - Added requirement to bind the X11 forwarding server to the loopback address.

SOL-11.1-060130

SOL-11.1-060130 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

SOL-11.1-070150

SOL-11.1-070150 - Updated Check Content command.

Solaris 11 X86 STIG Benchmark, Version 2, Release 2

NA

Rebundled to capture the changes to the STIG including updated rule IDs.

Solaris 11 x86 STIG, Version 2, Release 2

SOL-11.1-020540

SOL-11.1-020540 - Updated Check Content to remove unnecessary verbiage.

SOL-11.1-040010

SOL-11.1-040010 - Updated requirement to incorporate an increased granularity in password management.

SOL-11.1-040030

SOL-11.1-040030 - Updated requirement to incorporate an increased granularity in password management.

SOL-11.1-040331

SOL-11.1-040331 - Added requirement to bind the X11 forwarding server to the loopback address.

SOL-11.1-060130

SOL-11.1-060130 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

SOL-11.1-070150

SOL-11.1-070150 - Updated Check Content command.

SUSE Linux Enterprise Server (SLES) 12 STIG, Version 2, Release 2

SLES-12-010660

SLES-12-010660 - Removed this requirement because it is not a technical control.

SLES-12-010710

SLES-12-010710 - Updated Check Content command.

SLES-12-010730

SLES-12-010730 - Updated Check Content command.

SLES-12-010740

SLES-12-010740 - Updated Check Content command.

SLES-12-010750

SLES-12-010750 - Updated Check Content command.

SLES-12-010790

SLES-12-010790 - Updated Check Content command.

SLES-12-010850

SLES-12-010850 - Updated Check Content command.

SLES-12-020250

SLES-12-020250 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020260

SLES-12-020260 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020280

SLES-12-020280 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020310

SLES-12-020310 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020320

SLES-12-020320 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020550

SLES-12-020550 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020560

SLES-12-020560 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020570

SLES-12-020570 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020580

SLES-12-020580 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020600

SLES-12-020600 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020610

SLES-12-020610 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020620

SLES-12-020620 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020630

SLES-12-020630 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020640

SLES-12-020640 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020670

SLES-12-020670 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020680

SLES-12-020680 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020690

SLES-12-020690 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020700

SLES-12-020700 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020710

SLES-12-020710 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-020720

SLES-12-020720 - Updated aid from 500 to 1000 in Check and Fix Text.

SLES-12-030170

SLES-12-030170 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

SLES-12-030180

SLES-12-030180 - Updated Vulnerability Discussion, Check Content, and Fix Content to reflect cipher order requirement.

SLES-12-030191

SLES-12-030191 - Fixed typos in the Vulnerability Discussion and Check Content.

SLES-12-030260

SLES-12-030260 - Updated Rule Title, Vulnerability Discussion, Check Content, Fix Content to disable X11Forwarding and downgraded requirement to a CAT II.

SLES-12-030261

SLES-12-030261 - Added requirement to bind the X11 forwarding server to the loopback address.

TANS-SV-000001 - Modified fix criteria to add setting requirement for StateProtectedFlag value.

Virtual Private Network (VPN) SRG, Version 2, Release 2

SRG-NET-000375-VPN-001690

SRG-NET-000375-VPN-001690 - Changed "must use" to "does not enable" in the Check to make a finding if the encapsulation is not enabled.

VMware vSphere 6.5 ESXi STIG, Version 2, Release 1

ESXI-65-000078

ESXI-65-000078 - Modified to state any approved certificate.

VMware vSphere 6.5 vCenter Server for Windows STIG, Version 2, Release 1

VCWN-65-000058

VCWN-65-000058 - Modified to state any approved certificate.

Voice Video Endpoint SRG, Version 2, Release 1

SRG-NET-000140-VVEP-00032

SRG-NET-000140-VVEP-00032 - Changed N/A statement for hardware endpoint device multifactor authentication.

z/OS SRR Scripts, Version 6, Release 48

NA

Corrected error in scripts.
Corrected scripts to initialize variables.
Removed alias collection scripts and JCL.

ACF2-SM-000050

Corrected problem with findings for * access READ.

RACF-SM-000040

Corrected problem with findings for * access READ.

TSS0-SM-000010

Corrected problem with findings for * access READ.

z/OS STIG Instruction document, Version 6, Release 48

NA

Removed alias collection scripts and JCL.