OCTOBER 2017 MAINTENANCE RELEASE: STIGS TO BE RELEASED

AIX 6.1 STIG, Version 1, Release 11

V-12765

Updated the requirement text, check, and fix to remove the "DoD approved" wording.

Apache 2.2 Server UNIX STIG, Version 1, Release 9

V-26299

Added check content regarding a web server providing only a proxy server role.

Apache 2.2 Server WIN STIG, Version 1, Release 12

V-2235

Modified check criteria to validate documentation to reflect web service account password must be changed at least annually.

V-2243

Modified check and fix criteria to require a diagram showing clear location of private web server.

V-2248

Updated check content WRT web administrator roles.

V-13734

Modified Vulnerability Discussion and check content for clarity on the syntax of the Options directive.

V-13735

Modified Vulnerability Discussion and check content for clarity on the syntax of the Options directive.

Apache 2.2 Site WIN STIG, Version 1, Release 12

V-26281

Provided clarity to command string in check content.

Apache 2.2 WIN STIG, Version 1, Release 12

Documentation Update

Updated Overview Section 2.2 "Assumptions" WRT web administrator roles.

Application Core SRG, Version 2, Release 5

V-26978

Updated discussion to reflect "non-privileged accounts" as per CCI-000768.

Application Security and Dev STIG, Version 4, Release 4

V-69349

Updated check for 000550, added the following. "If the application has no interactive user interface, this requirement is not applicable."

Changed from CAT II to CAT III.

V-69351

Updated check for 000560, added the following. "If the only way to access the application is through the OS console, e.g., a fat client application installed on a GFE desktop or laptop, and that GFE is configured to display the DoD banner, an additional banner is not required at the application level."

V-70147

Updated vul discussion: "The application must ensure that a user does not retain any rights that may have been granted prior to the change or access to the application after the user's authorization or role within the application has been deleted or modified. This means once a user's role/account within the application has been modified, deleted or disabled, the changes must be enforced immediately within the application. Any privileges or access the user had prior to the change must not be retained. For example; any application sessions that the user may have already established prior to the configuration change must be terminated when the user account changes occur. "

V-70425

Changed the CCI from CCI-001567 to CCI-002052.

BlackBerry OS 7.x STIG, Version 2, Release 11

V-76833

Added check to sunset STIG.

Documentation Update

Updated format of all STIG documents. Updated Revision History document.

Cisco IOS XE Release 3 NDM STIG, Version 1, Release 3

V-73973

Update the check and fix content to appear as follows: login block-for 600 attempts 3 within 900.

DNS Policy STIG, Version 4, Release 1-21

V-13036

Updated with verbiage WRT web administrator roles.

Firewall STIG - Cisco, Version 8, Release 24

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Good for Enterprise 8.x STIG, Version 1, Release 2

V-53153

Fixed text error in check.

V-76677

Added check to sunset STIG.

Documentation Update

Updated format of all STIG documents. Added Revision History document to STIG package.

Google Chrome Browser STIG, Version 1, Release 10

V-44741

Update policy name to "Enable saving passwords to the password manager".

V-44769

Update policy name to "Do not predict network actions on any network connection".

V-44805

Rewrite check to simply state "The version of Chrome must be the latest available" effectively removing auto-update function (We don't let any other app do this).

Google Chrome for Windows Benchmark, Version 1, Release 5

Benchmark Update

Repackaged benchmark for updated Rule IDs.

HP-UX 11.31 Benchmark, Version 1, Release 15

V-924

Added /dev/syscon to the devices excluded from the check.

V-960

Updated OVAL to check for existence of /etc/shadow.

V-22413

Updated OVAL to accept "all" in ipf.conf, in addition to "from any to any".

V-22414

Updated OVAL to accept "all" in ipf.conf, in addition to "from any to any".

HPUX 11.31 STIG, Version 1, Release 15

V-12765

Updated the requirement text, check, and fix to remove the "DoD approved" wording.

IBM DataPower Network Device Management STIG, Version 1, Release 2

V-65121

Change SSH Proxy Profile to SSH Client Profile with was an error in the procedure.

V-65123

Change SSH Proxy Profile to SSH Client Profile with was an error in the procedure.

IBM Hardware Management Console (HMC) STIG, Version 1, Release 5

Documentation Update

Repackaged STIG.

IIS 7.0 STIG, Version 1, Release 15

V-2240

Update the check content and fix text for V-2240 to reflect the following path: "\Windows\system32\inetsrv".

V-2252

Was going to sync permissions with V-13689, but this creates a redundant check. V-13689 covers the intent of both, so removing V-2252.

V-2262

Remove "FIPS 140-2 approved TLS versions include TLS V1.0 or greater" from Vul Disc.
Check content and fix text should say SSL settings.

V-6531

Check content and fix text should say SSL settings.

V-6755

Check should say Actions Pane and not Alerts Pane.

V-13688

Change "If not, this is a finding." to "If logging is not enabled, this is a finding."

V-13689

Step 4 should say Beside Directory click Browse. Remove first note.

V-13704

Add a NOTE that states "DO NOT CLICK Recycle!".

Infrastructure L3 Switch STIG - Cisco, Version 8, Release 24

V-3080

Updated entire check to allow for Configuration auto-loading when not connected to an operational network.

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Infrastructure L3 Switch STIG, Version 8, Release 24

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Documentation Update

Updated release number.

Infrastructure Router STIG - Cisco, Version 8, Release 24

V-3080

Updated entire check to allow for Configuration auto-loading when not connected to an operational network.

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Infrastructure Router STIG - Juniper, Version 8, Release 24

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Documentation Update

Updated release number.

Infrastructure Router STIG, Version 8, Release 24

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Documentation Update

Updated release number.

IPSec VPN Gateway STIG, Version 1, Release 13

V-3080

Updated entire check to allow for Configuration auto-loading when not connected to an operational network.

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

JIE CDC STIG, Version 2, Release 3

V-59457

Reword the vulnerability discussion to clarify the requirement.

V-59459

Reword the vulnerability discussion to clarify the requirement.

V-59463

Focused this CAT 1 requirement so there is a CAT 1 finding for not having an AAF in the Core Zone security Stack rather than mixing with intra-zone communications for Security Tiers.

V-77829

Created this new CAT 2 requirement that focuses on configuring the Zone AAF to monitor intra-zone communications at the entry points of the Security Tiers and subzones.

JIE IPN STIG, Version 2, Release 3

V-59393

Reword the vulnerability discussion to clarify the requirement.

V-59395

Reword the vulnerability discussion to clarify the requirement.

V-59399

Focused this CAT 1 requirement so there is a CAT 1 finding for not having an AAF in the Core Zone security Stack rather than mixing with intra-zone communications for Security Tiers.

V-77817

Created this new CAT 2 requirement that focuses on configuring the Zone AAF to monitor intra-zone communications at the entry points of the Security Tiers and subzones.

Juniper SRX SG VPN STIG, Version 1, Release 2

V-66649

Update the Fix text for this rule says “set security ike …” when it should say “set security ipsec …”. The “Check Content” tab correctly references the “set security ipsec”.

Layer 2 Switch STIG - Cisco, Version 8, Release 22

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Layer 2 Switch STIG, Version 8, Release 22

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

McAfee Application Control 7.x STIG, Version 1, Release 2

V-74217

Modified check content WRT GTI and classified networks.

V-74243

Modified requirement, vulnerability discussion, check and fix content to be consist with HBSS PMO's published best practices.

McAfee VSEL 1.9/2.0 Managed Client STIG, Version 1, Release 3

V-63017

Modified finding statement for clarity.

V-63033

Correct last finding statement in check criteria.

V-63049

Modified requirement for approved excluded paths to be consistent with best practices.

V-63059

Modified check and fix criteria to be more specific relating to paths being scanned.

V-63061

Modified the vulnerability discussion to be consistent with vulnerability of requirement.

MS Access 2007 STIG, Version 4, Release 15

V-25884

Add CAT I check, validate if running MS Access 2007, sunset STIG.

MS Excel 2007 STIG, Version 4, Release 13

V-25884

Add CAT I check, validate if running MS Excel 2007, sunset STIG.

MS Excel 2016 Benchmark, Version 1, Release 2

Benchmark Update

Repackaged benchmark for updated Rule IDs.

MS Excel 2016 STIG, Version 1, Release 2

V-70983

Corrected typo in fix text, from Excel 20163 to Excel 2016.

MS InfoPath 2007 STIG, Version 4, Release 13

V-25884

Add CAT I check, validate if running MS InfoPath 2007, sunset STIG.

MS Office 2007 STIG, Version 4, Release 15

V-25884

Modify to CAT I, validate if running Office System 2007, sunset Office 2007 suite.

MS Outlook 2007 STIG, Version 4, Release 16

V-17559

In check content, correct registry validation to reflect correct key and value.

V-17733

In check content, correct registry validation to reflect correct key and value.

V-17774

In check content, correct registry validation to reflect correct key and value.

V-17775

In check content, correct registry validation to reflect correct key and value.

V-25884

Add CAT I check, validate if running MS Outlook 2007, sunset STIG.

MS Outlook 2013 Benchmark, Version 1, Release 6

Benchmark Update

Repackaged benchmark for updated Rule IDs.

MS Outlook 2013 STIG, Version 1, Release 11

V-17760

Correct administrative template path in fix text to read "MS Outlook 2013" instead of "MS Outlook 2010".

V-17774

Modified registry path/key/value for clarification.

V-17775

Modified registry path/key/value for clarification.

MS Outlook 2016 Benchmark, Version 1, Release 3

Benchmark Update

Repackaged benchmark for updated Vulnerability Discussions.

MS PowerPoint 2007 STIG, Version 4, Release 16

V-25884

Add CAT I check, validate if running MS PowerPoint 2007, sunset STIG.

MS Windows 10 Mobile STIG, Version 1, Release 3

V-70097

Changed technical procedure to implement requirement since Windows 10 Mobile now supports removable media encryption.

V-70099

OS update policy and procedures were modified.

V-70133

Removed Allow User Decryption policy rule from the requirement. The control is no longer supported in Windows 10 mobile.

V-70141

OS no longer supports this function. Requirement included in MSWM-10-911101.

V-71681

Revised minimum required OS version.

Documentation Update

Updated format of all STIG documents. Updated Revision History document.
Revised Section 2.2 of the Supplemental document.

MS Word 2007 STIG, Version 4, Release 15

V-25884

Add CAT I check, validate if running MS Word 2007, sunset STIG.

Network Device Management SRG, Version 2, Release 12

V-68747

Added missing CCI to SRG-APP-000395-NDM-000347. Added CCI-001967.

Documentation Update

History for V2R7, change “V-55401”. STIG ID of SRG-APP-000025-NDM-000207 read “V-55041 in place of “V-55401”?

Network Infrastructure Policy STIG, Version 9, Release 4

V-11796

Corrected the discussion section by removing the last sentence.

Oracle HTTP Server STIG, Version 1, Release 2

V-64465

Changed check language to match fix language. "Set the"LimitRequestBody" directive to a value of "10240".

Oracle JRE 8 UNIX STIG, Version 1, Release 3

V-66909

Remove the syntax "file://".

Oracle Linux 6 STIG, Version 1, Release 11

V-50689

Based on the recommendation from the Oracle Linux engineering team, the check has been refined to produce more accurate results.

V-50873

Updated the requirement text, check, and fix to remove the "DoD approved" wording. Lowered the severity of the requirement to a CAT II to be consistent with other guidance.

Oracle WebLogic Server 12c STIG, Version 1, Release 3

V-56213

Corrected the URL to: https://iase.disa.mil/ppsm/Pages/index.aspx.

V-56273

Corrected the URL to: https://iase.disa.mil/ppsm/Pages/index.aspx.

Perimeter L3 Switch STIG - Cisco, Version 8, Release 27

V-3080

Updated entire check to allow for Configuration auto-loading when not connected to an operational network.

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Perimeter L3 Switch STIG, Version 8, Release 27

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Documentation Update

Updated release number.

Perimeter Router STIG - Cisco, Version 8, Release 27

V-3080

Updated entire check to allow for Configuration auto-loading when not connected to an operational network.

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Perimeter Router STIG - Juniper, Version 8, Release 27

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Documentation Update

Updated release number.

Perimeter Router STIG, Version 8, Release 27

V-3085

Updated the discussion section to clarified the difference between enabling HTTP and HTTPS services for administrative access.

Documentation Update

Updated release number.

Red Hat 5 Benchmark, Version 1, Release 19

Benchmark Update

Rebundle to update Benchmark version.

Red Hat 6 Benchmark, Version 1, Release 17

V-38513

Corrected an error in an OVAL regular expression.

V-38520

Added "@@" to OVAL as an acceptable indicator of a remote syslog server.

V-38521

Added "@@" to OVAL as an acceptable indicator of a remote syslog server.

Red Hat 6 STIG, Version 1, Release 17

V-38490

Added a “grep” statement to eliminate any configurations that are commented out from appearing in the returned results list.

V-38514

Added a “grep” statement to eliminate any configurations that are commented out from appearing in the returned results list.

V-38515

Added a “grep” statement to eliminate any configurations that are commented out from appearing in the returned results list.

V-38517

Added a “grep” statement to eliminate any configurations that are commented out from appearing in the returned results list.

V-38666

Updated the requirement text, check, and fix to remove the "DoD approved" wording. Lowered the severity of the requirement to a CAT II to be consistent with other guidance.

V-38679

Added a “Not Applicable” statement for systems that are utilizing DHCP. Updated the check content to be more in-line with the requirement.

V-38682

Added a “grep” statement to eliminate any configurations that are commented out from appearing in the returned results list.

V-58901

Added a "Not Applicable" statement for systems that do not utilize passwords for authentication.

Red Hat Enterprise Linux 7 STIG, Version 1, Release 3

V-71861

Updated the banner text to include formatting for proper display in a GUI.

V-71891

Removed the requirement to set "lock-delay=uint32 180".

V-71893

Removed the requirement to set "lock-delay=uint32 180".

V-71899

Corrected dashes in the command in the Check instructions.

V-71905

Updated the fix text to match the requirement.

V-71915

Updated the number of characters that are required.

V-71919

Updated the fix text to state that the "authconfig" program should not be used when making manual updates.

V-71933

Updated the fix text to state that the "authconfig" program should not be used when making manual updates.

V-71937

Updated the fix text to state that the "authconfig" program should not be used when making manual updates.

V-71943

Updated the check and fix to require the use of "account required pam_faillock.so". Updated the fix text to state that the "authconfig" program should not be used when making manual updates.

V-71945

Added the "unlock_time" variable to the check content, updated the check and fix to require the use of "account required pam_faillock.so", and updated the fix text to state that the "authconfig" program should not be used when making manual updates.

V-71947

Added a "Not Applicable" statement for systems that do not utilize passwords for authentication.

V-71961

Added a "Not Applicable" statement for systems that utilize UEFI.

V-71963

Added a "Not Applicable" statement for systems that utilize BIOS.

V-72035

Updated the fix text to match the requirement.

V-72041

Updated the check to include the 3rd field and adjusted the example output to match.

V-72047

Moved the "-xdev" option in front of the "-perm" option to eliminate a warning that was being issued by the find command.

V-72063

Updated the check content to match the requirement.

V-72079

Updated the Fix text to utilize "systemctl" command.

V-72081

Updated the check and fix to utilize the correct options in the audit.rules file.

V-72095

Updated the fix to utilize the "path=" option and updated the example output in the check to match.

V-72141

Updated Check and Fix commands and altered text to address "setfiles".

V-72145

Removed excessive whitespace from the listed audit rule in the fix text.

V-72163

Updated the "grep" statements in the Check content. Updated the audit rule for "/etc/sudoers.d/" in the fix text.

V-72169

Updated the "grep" statement in the check content.

V-72171

Updated the "grep" statement in the check content to search for "mount" as "/bin/mount" does not appear in the defined audit rule.

V-72173

Updated the "grep" statement in the check content.

V-72185

Updated the "grep" statement in the check content.

V-72191

Removed the note about appropriate architecture from the check and fix.

V-72193

Removed the note about appropriate architecture from the check and fix.

V-72195

Removed the note about appropriate architecture from the check and fix.

V-72197

Updated the key used in the audit rule to "identity".

V-72213

Updated language related to antivirus software requirements.

V-72215

Updated language related to antivirus software requirements.

V-72223

Updated the check and fix to allow for the use of a shell script in lieu of adding the required settings directly to the /etc/bashrc file.

V-72225

Removed the "=" from the banner configuration line.

V-72233

Updated the "yum" command to utilize a "grep" command.

V-72305

Updated the check to focus solely on the "tftp-server" package.

V-72307

Updated the check content to use "rpm" versus "yum" due to "rpm" producing more accurate results.

V-72315

Updated the check and fix content to differentiate between the use of firewalld and tcpwrappers.

V-72433

Corrected "ocsp" reference.

V-73167

Updated the key used in the audit rule to "identity".

V-73171

Updated the key used in the audit rule to "identity".

V-73173

Updated the requirement to utilize the correct path for /etc/security/opasswd. Updated the key used in the audit rule to "identity".

V-73175

Updated the finding statement to remove the reference to multiple results resulting from the check command.

V-77819

Added a requirement for multifactor authentication when utilizing a GUI.

V-77821

Added a new requirement to disable the Datagram Congestion Control Protocol (DCCP) kernel module.

V-77823

Added a new requirement to enforce the use of authentication when booting into single-user and maintenance modes.

V-77825

Added a requirement for the use of virtual address space randomization.

Removable Storage and External Connections STIG, Version 1, Release 7

V-23920

Removed reference to outdated software - File Sanitization Tool (FiST) and Magik Eraser (ME).

V-23921

Removed reference to outdated software - File Sanitization Tool (FiST) and Magik Eraser (ME).

SLES V11 for System Z STIG, Version 1, Release 11

V-12765

Updated the requirement text, check, and fix to remove the "DoD-approved" wording.

Solaris 10 SPARC Benchmark, Version 1, Release 19

V-907

Updated OVAL to verify existence of PATH variables before checking them for null values.

Solaris 10 SPARC STIG, Version 1, Release 20

V-12765

Updated language related to antivirus software requirements.

Solaris 10 X86 Benchmark, Version 1, Release 19

V-907

Updated OVAL to verify existence of PATH variables before checking them for null values.

Solaris 10 x86 STIG, Version 1, Release 20

V-12765

Updated language related to antivirus software requirements.

Solaris 11 SPARC Benchmark, Version 1, Release 8

V-59831

Updated OVAL to verify existence of PATH variables before checking them for null values.

Solaris 11 SPARC STIG, Version 1, Release 13

V-47955

Updated language related to antivirus software requirements.

V-47959

Updated language related to antivirus software requirements.

V-47963

Updated language related to antivirus software requirements.

Solaris 11 X86 Benchmark, Version 1, Release 8

V-59831

Updated OVAL to verify existence of PATH variables before checking them for null values.

Solaris 11 X86 STIG, Version 1, Release 13

V-47955

Updated language related to antivirus software requirements.

V-47959

Updated language related to antivirus software requirements.

V-47963

Updated language related to antivirus software requirements.

Voice Video Endpoint SRG, Version 1, Release 6

V-77277

Add Requirement SRG-NET-000494-VVEP-00061 to produce session (call detail) records containing classification level and SAL.

V-77281

Add Requirement SRG-NET-000311-VVEP-00062 to properly mark hardware endpoints with highest classification level. (DRSN 1098)

V-77283

Add Requirement SRG-NET-000311-VVEP-00063 for secure endpoints to display classification, SAL, and user identity. (DRSN 2384/2385)

Windows 2008 DC Benchmark, Version 6, Release 40

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 2008 DC.

V-73523

Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found and not specifically for other defaults.

Windows 2008 DC STIG, Version 6, Release 38

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26683

Clarified various formats may exist for individual identifiers.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-39332

Clarified changes from schema update to support Exchange are not a finding.

V-73523

Modified Check to only be a finding if SMBv1 is found.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 2008 MS Benchmark, Version 6, Release 40

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 2008 MS.

V-73523

Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found and not specifically for other defaults.

Windows 2008 MS STIG, Version 6, Release 38

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-73523

Modified Check to only be a finding if SMBv1 is found.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 2008 R2 DC Benchmark, Version 1, Release 26

V-26475

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26477

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26502

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26505

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 2008 R2 DC.

V-73523

Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found and not specifically for other defaults.

Windows 2008 R2 DC STIG, Version 1, Release 24

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26475

Removed user right requirement that does not provide security benefit, Bypass traverse checking.

V-26477

Removed user right requirement that does not provide security benefit, Change the time zone.

V-26502

Removed user right requirement that does not provide security benefit, Remove computer from docking station.

V-26505

Removed user right requirement that does not provide security benefit, Shut down the system.

V-26683

Clarified various formats may exist for individual identifiers.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-39332

Clarified changes from schema update to support Exchange are not a finding.

V-73519

Updated Fix to use custom administrative template for configuration.

V-73523

Modified Check to only be a finding if SMBv1 is found. Updated Fix to use custom administrative template for configuration.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 2008 R2 MS Benchmark, Version 1, Release 27

V-26475

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26477

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26502

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26505

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 2008 R2 MS.

V-73523

Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found and not specifically for other defaults.

Windows 2008 R2 MS STIG, Version 1, Release 24

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26475

Removed user right requirement that does not provide security benefit, Bypass traverse checking.

V-26477

Removed user right requirement that does not provide security benefit, Change the time zone.

V-26502

Removed user right requirement that does not provide security benefit, Remove computer from docking station.

V-26505

Removed user right requirement that does not provide security benefit, Shut down the system.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-73519

Updated Fix to use custom administrative template for configuration.

V-73523

Modified Check to only be a finding if SMBv1 is found. Updated Fix to use custom administrative template for configuration.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 2012/2012 R2 DC Benchmark, Version 2, Release 10

V-26475

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26477

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26505

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 2012 and 2012 R2 DC.

V-43239

Updated the OVAL content to allow "Include command line in process creation events" policy to be set to "Enabled".

V-73519

Updated the OVAL content for SMBv1 Server requirement to pass on Windows Server 2012 R2.

V-73523

Updated the OVAL content for SMBv1 Client requirement to pass on Windows Server 2012 R2. Updated DependOnService to be a finding only if SMBv1 is found and not specifically for other defaults.

V-73805

Updated the OVAL content for SMBv1 Protocol requirement to allow a combination of the V-73519 and V-73523 fixes to close the requirement.

Windows 2012/2012 R2 DC STIG, Version 2, Release 10

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26475

Removed user right requirement that does not provide security benefit, Bypass traverse checking .

V-26477

Removed user right requirement that does not provide security benefit, Change the time zone.

V-26505

Removed user right requirement that does not provide security benefit, Shut down the system.

V-26683

Clarified various formats may exist for individual identifiers.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-36774

Removed requirement for a specific screen saver, no security benefit.

V-36775

Removed requirement to prevent screen saver change, no security benefit.

V-39332

Clarified changes from schema update to support Exchange are not a finding.

V-43239

Changed requirement to enable command line data to be included in process creation events.

V-57653

Clarified applicability of requirement for temporary accounts.

V-57655

Clarified applicability of requirement for emergency administrative accounts.

V-73519

Updated Fix to use custom administrative template for configuration.

V-73523

Modified Check to only be a finding if SMBv1 is found. Updated Fix to use custom administrative template for configuration.

V-73805

Updated to allow alternate method for disabling SMBv1.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 2012/2012 R2 MS Benchmark, Version 2, Release 10

V-26475

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26477

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26505

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 2012 and 2012 R2 MS.

V-43239

Updated the OVAL content to allow "Include command line in process creation events" policy to be set to "Enabled".

V-73519

Updated the OVAL content for SMBv1 Server requirement to pass on Windows Server 2012 R2.

V-73523

Updated the OVAL content for SMBv1 Client requirement to pass on Windows Server 2012 R2. Updated DependOnService to be a finding only if SMBv1 is found and not specifically for other defaults.

V-73805

Updated the OVAL content for SMBv1 Protocol requirement to allow a combination of the V-73519 and V-73523 fixes to close the requirement.

Windows 2012/2012 R2 MS STIG, Version 2, Release 10

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26475

Removed user right requirement that does not provide security benefit, Bypass traverse checking .

V-26477

Removed user right requirement that does not provide security benefit, Change the time zone.

V-26505

Removed user right requirement that does not provide security benefit, Shut down the system.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-36774

Removed requirement for a specific screen saver, no security benefit.

V-36775

Removed requirement to prevent screen saver change, no security benefit.

V-43239

Changed requirement to enable command line data to be included in process creation events.

V-57653

Clarified applicability of requirement for temporary accounts.

V-57655

Clarified applicability of requirement for emergency administrative accounts.

V-73519

Updated Fix to use custom administrative template for configuration.

V-73523

Modified Check to only be a finding if SMBv1 is found. Updated Fix to use custom administrative template for configuration.

V-73805

Updated to allow alternate method for disabling SMBv1.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 7 Benchmark, Version 1, Release 34

V-26475

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26477

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26502

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26505

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-28285

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-32282

Adapt the existing Windows 8 OVAL content for V-32282 to create the new OVAL content for Windows 7.

V-73523

Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found and not specifically for other defaults.

Windows 7 STIG, Version 1, Release 28

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26475

Removed user right requirement that does not provide security benefit, Bypass traverse checking.

V-26477

Removed user right requirement that does not provide security benefit, Change the time zone.

V-26502

Removed user right requirement that does not provide security benefit, Remove computer from docking station.

V-26505

Removed user right requirement that does not provide security benefit, Shut down the system.

V-28285

Removed user right requirement that does not provide security benefit, Log on as a service.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-73519

Updated Fix to use custom administrative template for configuration.

V-73523

Modified Check to only be a finding if SMBv1 is found. Updated Fix to use custom administrative template for configuration.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows 8/8.1 Benchmark, Version 1, Release 20

V-26475

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26477

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26502

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-26505

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-28285

Removed OVAL content from the benchmark as the requirement has been removed from the STIG.

V-43239

Updated OVAL content for the Audit Process Creation requirement to be used by Windows Server 2012.

V-73519

Added new OVAL content for the SMBv1 Server requirement.

V-73523

Added new OVAL content for the SMBv1 Client requirement.

V-73805

Updated the OVAL content for SMBv1 Protocol requirement to allow a combination of the V-73519 and V-73523 fixes to close the requirement.

Windows 8/8.1 STIG, Version 1, Release 19

V-1074

Removed specific antivirus product referenced.

V-1089

Removed short version of banner text as NA.

V-26475

Removed user right requirement that does not provide security benefit, Bypass traverse checking.

V-26477

Removed user right requirement that does not provide security benefit, Change the time zone.

V-26502

Removed user right requirement that does not provide security benefit, Remove computer from docking station.

V-26505

Removed user right requirement that does not provide security benefit, Shut down the system.

V-28285

Removed user right requirement that does not provide security benefit, Log on as a service.

V-32272

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-73519

Added as alternate method for disabling SMBv1 server.

V-73523

Added as alternate method for disabling SMBv1 client.

V-73805

Updated to allow alternate method for disabling SMBv1.

V-75915

Added requirement for unresolved SIDs found on user rights.

Windows Server 2016 Benchmark, Version 1, Release 3

V-73297

Added new OVAL content.

V-73301

Added new OVAL content.

V-73443

Added new OVAL content.

V-73445

Added new OVAL content.

V-73477

Added new OVAL content.

V-73479

Added new OVAL content.

V-73493

Added OVAL to verify the display of slide shows on the lock screen is disabled.

V-73497

Added OVAL to verify WDigest authentication is disabled.

V-73507

Added OVAL to verify insecure SMB logons are disabled.

V-73509

Added OVAL to verify hardened UNC paths are defined to require mutual authentication and integrity for specified shares.

V-73511

Added new OVAL content for the Audit Process Creation requirement.

V-73531

Added OVAL to verify the network selection UI is disabled on the logon screen.

V-73551

Added OVAL to verify configuration of Windows Telemetry.

V-73581

Added OVAL to verify indexing of encrypted files is turned off.

V-73589

Added OVAL to verify automatic sign-in for the last interactive user before a restart is disabled.

V-73591

Added OVAL to verify PowerShell script block logging is enabled.

z/OS Automated PDI list spreadsheet, Version 6, Release 33

V-6997

Changes made to indicate STIG ID is automated.

V-17067

Changes made to indicate STIG ID is automated.

V-75057

Changes made to indicate STIG ID is automated.

z/OS Cross Ref of SRRAUDIT spreadsheet, Version 6, Release 33

V-17067

Changes added data set requirement for STIG ID.

V-17947

Changed spreadsheet adding new resources and the access requirements identified in ticket.

z/OS PDI list spreadsheet, Version 6, Release 33

V-6997

Changes made to indicate STIG ID is automated.

V-17067

Changes made to indicate STIG ID is automated.

V-75057

Changes made to indicate STIG ID is automated.

z/OS SRR Scripts, Version 6, Release 33

V-6993

Changed scripts to reflect changes that are documented in ticket.

V-6997

Changed scripts to reflect changes that are documented in ticket. New automation.

V-7000

Changed scripts to reflect changes that are documented in ticket.

V-17067

Changed scripts to reflect changes that are documented in ticket. New automation.

V-17947

Changed scripts to add resources that are documented in ticket.

V-19893

Changed scripts to information collected before script analysis of results.

V-75057

Changed scripts to reflect changes that are documented in ticket. New automation.

z/OS SRRAUDIT Dialog Management document, Version 6, Release 33

V-17067

Changes made to document to add dialog panel to collect STC data sets.

zOS ACF2 STIG, Version 6, Release 33

V-3216

Update Check to indicate that DOMAINORIGIN or DOMAIN is allowed.

Documentation Update

Update access levels in Addendum and Cross reference.

zOS BMC CONTROL-M for RACF STIG, Version 6, Release 7

Documentation Update

Repackaged STIG.

zOS BMC CONTROL-M for TSS STIG, Version 6, Release 7

Documentation Update

Repackaged STIG.

zOS BMC MAINVIEW for ACF2 STIG, Version 6, Release 5

V-17452

Remove MAINVIEW requirement for the use of MUSASS it is no longer needed for their started tasks.

zOS CLSupersession for ACF2 STIG, Version 6, Release 9

Documentation Update

Repackaged STIG.

zOS CLSupersession for RACF STIG, Version 6, Release 9

Documentation Update

Repackaged STIG.

zOS CLSupersession for TSS STIG, Version 6, Release 9

Documentation Update

Repackaged STIG.

zOS CSSMTP for ACF2 STIG, Version 6, Release 5

V-17067

Add statement to the checks of ZSMT0001 to specify automation is available.

zOS CSSMTP for RACF STIG, Version 6, Release 5

V-17067

Add statement to the checks of ZSMT0001 to specify automation is available.

zOS CSSMTP for TSS STIG, Version 6, Release 5

V-17067

Add statement to the checks of ZSMT0001 to specify automation is available.

zOS RACF STIG, Version 6, Release 33

V-3216

Update Check to indicate that DOMAINORIGIN or DOMAIN is allowed.

V-6997

Add statement to the check of ZUSSR050 to specify automation is available:

V-75057

Add statement to the check of ITCPR052 to specify automation is available.

Documentation Update

Update access levels in Addendum and Cross reference.

zOS TSS STIG, Version 6, Release 33

V-3216

Update Check to indicate that DOMAINORIGIN or DOMAIN is allowed.

Documentation Update

Update access levels in Addendum and Cross reference.