STIG SUMMARY
LAST UPDATED: MARCH 13, 2020

This document lists:

- All STIG updates included in the quarterly STIG release
- Out-of-cycle STIG changes made between quarterly releases
- Additional STIG-related postings to or removals from Cyber Exchange between quarterly releases

---

CONTENTS **PAGE**

STIG UPDATES – OUT-OF-CYCLE

HBSS ePO 5.x STIG, Version 1, Release 20
V-14484 - Expanded text to explain "DoD boundary". V-14493 - Corrected STIG check criteria to remove outdated patches repository link. V-14497 - Added caveat to requirement to allow any software to be installed on ePO server, providing it is required specifically by another STIG applicable to the ePO server (i.e., the OS STIG). V-14519 – Reworded “Note” text in check to clarify. V-14939 - Revised account list of those with access to the ePO database. V-24175 - Added note to specify requirement is Not Applicable if ePO is the only Agent Handler. V-31094 - Reworded check criteria to indicate that exceptions must be handled via a configuration management plan. All requirements - Renamed all STIG IDs from -ePO 5.3/5.9 to -ePO 5x.
Microsoft Windows 10 STIG, Version 1, Release 20
V-63323 - Upgraded severity level from CAT III to CAT II. V-63349 - Revised required version to Windows Version 1709 or greater. V-63441 - Removed requirement to configure the system to audit Account Management - Other Account Management Events successes. V-63455 - Removed requirement to configure the system to audit Logon/Logoff - Account Lockout successes. V-63475 - Removed requirement to configure the system to audit Policy Change - Audit Policy Change failures. V-63495 - Removed requirement for Audit IPsec Driver Audit Success. V-63587 - Changed wording. "If an expired certificate is found, this is a finding." V-63589 - Changed wording. "If an expired certificate is found, this is a finding." V-63599 - Changed Windows 10 Credential Guard requirement severity to CAT I. V-63607 - Revised rule title to prevent boot drivers, not just those identified as bad, and revised configuration instructions. V-63705 - Removed requirement to allow InPrivate browsing Disabled.

V-63707 - Remove requirement for Microsoft network client: Digitally sign communications (if server agrees) Success.
V-63723 - Removed requirement for SMB packet signing.
V-63763 - Removed requirement for Network security: Allow Local System to use computer identity for NTLM.
V-63887 - Removed requirement that generate security audits user right must only be assigned to Local Service and Network Service.
V-63891 - Removed requirement to increase scheduling priority.
V-72769 - Changed Check Text "This is NA if the system does not have Bluetooth, or if Bluetooth is turned off per the organizations policy."
V-74415 - Removed requirement to allow clearing browsing data on exit.
V-77189 - Changed Exploit Protection setting for Windows 10 Acrobat.exe.
V-77191 - Changed Exploit Protection setting for Windows 10 AcroRd32.exe.
V-77195 - Changed Exploit Protection setting for Windows 10 Chrome.exe.
V-77201 - Changed Exploit Protection setting for Windows 10 Excel.exe.
V-77205 - Changed Exploit Protection setting for Windows 10 Firefox.exe.
V-77209 - Changed Exploit Protection setting for Windows 10 FLTLDR.exe.
V-77213 - Changed Exploit Protection setting for Windows 10 Groove.exe.
V-77217 - Changed Exploit Protection setting for Windows 10 Iexplorer.exe.
V-77221 - Changed Exploit Protection setting for Windows 10 Infopath.exe.
V-77223 - Changed Exploit Protection setting for Windows 10 Java.exe.
V-77227 - Changed Exploit Protection setting for Windows 10 Lync.exe.
V-77231 - Changed Exploit Protection setting for Windows 10 Msaccess.exe.
V-77233 - Changed Exploit Protection setting for Windows 10 MSpub.exe.
V-77235 - Changed Exploit Protection setting for Windows 10 OneDrive.exe.
V-77239 - Changed Exploit Protection setting for Windows 10 OIS.exe.
V-77243 - Changed Exploit Protection setting for Windows 10 Outlook.exe.
V-77247 - Changed Exploit Protection setting for Windows 10 Powerpnt.exe.
V-77249 - Changed Exploit Protection setting for Windows 10 Pptview.exe.
V-77255 - Changed Exploit Protection setting for Windows 10 Visio.exe.
V-77259 - Changed Exploit Protection setting for Windows 10 Vpreview.exe.
V-77263 - Changed Exploit Protection setting for Windows 10 Winword.exe.
V-77267 - Changed Exploit Protection setting for Windows 10 Wmplayer.exe.
V-77269 - Changed Exploit Protection setting for Windows 10 Wordpad.exe.
V-88203 - Revised to WN10-CC-000340 to create a unique STIGID.
V-94861 - Added registry path to check text:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE
V-99541 - Added requirement to audit other Logon/Logoff Events - Failures.
V-99543 - Added requirement to audit other Logon/Logoff Events - Successes.
V-99545 - Added requirement to audit Detailed File Share - Failures.
V-99547 - Added requirement to audit MPSSVC Rule-Level Policy Change - Successes.
V-99549 - Added requirement to audit MPSSVC Rule-Level Policy Change - Failures.
V-99551 - Added requirement to audit Other Policy Change Events - Successes.
V-99553 - Added requirement to audit Other Policy Change Events - Failures.
V-99555 - Added requirement to change passwords for built-in local Administrator account at least every 60 days.
V-99557 - Added requirement to enable Windows 10 Kernel (Direct Memory Access) DMA Protection.
V-99559 - Added requirement to disable the convenience PIN for Windows 10.
V-99561 - Added requirement to configure Windows Ink Workspace to disallow access above the lock.
V-99563 - Added requirement to configure Window 10 to prevent users from receiving suggestions for third-party or additional applications.
Supporting files folder - Revised DOD_EP file.

Microsoft Windows 10 STIG Benchmark, Version 1, Release 17
Rebundled benchmark to accommodate updated Rule ID.
z/OS ACF2 Products, Version 6, Release 44
z/OS Front End Processor (FEP) STIG, zOS Websphere Application Server (WAS) STIG, z/OS WebsphereMQ STIG - Pulled from z/OS STIGs and packaged here. z/OS CICA Transaction Server - Pulled all CICA requirements from z/OS STIGs.
z/OS RACF Products, Version 6, Release 44
z/OS Front End Processor (FEP) STIG, zOS Websphere Application Server (WAS) STIG, z/OS WebsphereMQ STIG - Pulled from z/OS STIGs and packaged here. z/OS CICA Transaction Server - Pulled all CICA requirements from z/OS STIGs.
z/OS TSS Products, Version 6, Release 44
z/OS Front End Processor (FEP) STIG, zOS Websphere Application Server (WAS) STIG, z/OS WebsphereMQ STIG - Pulled from z/OS STIGs and packaged here. z/OS CICA Transaction Server - Pulled all CICA requirements from z/OS STIGs.
z/OS SRR Scripts, Version 6, Release 44
Revised Release number and date to align with z/OS Products packages; no other changes made.

NEW STIGS

BlackBerry UEM 12.11 STIG, Version 1, Release 1
Approved January 2, 2020
Jamf Pro v10.x EMM STIG, Version 1, Release 1
Approved February 9, 2020
Oracle Linux 7 STIG, Version 1, Release 1
Approved February 9, 2020
z/OS STIG, Version 7, Release 1
Approved November 18, 2019 (new version of z/OS ACF2, RACF, and TSS STIGs released with Version 6 of the z/OS Products files)

NEW STIG BENCHMARKS

Canonical Ubuntu STIG Benchmark - Ver 1, Rel 1
Benchmark Date: February 10, 2020
SUSE Linux Enterprise Server 12 STIG Benchmark - Ver 1, Rel 1
Benchmark Date: February 14, 2020
Oracle Linux 7 STIG Benchmark - Ver 1, Rel 1
Benchmark Date: February 10, 2020

STIGS SUNSET

Microsoft Windows 2008 DC STIG, Version 6, Release 45
V-1073 - Updated requirement to note that support for the OS has ended and systems must use Windows 2012 or greater.
Microsoft Windows 2008 DC STIG Benchmark, Version 6, Release 45
Rebundled benchmark to accommodate updated Rule ID.
Microsoft Windows 2008 MS STIG, Version 6, Release 44
V-1073 - Updated requirement to note that support for the OS has ended and systems must use Windows 2012 or greater.
Microsoft Windows 2008 MS STIG Benchmark, Version 6, Release 45
Rebundled benchmark to accommodate updated Rule ID.
Microsoft Windows 2008 R2 DC STIG, Version 1, Release 32
V-1073 - Updated requirement to note that support for the OS has ended and systems must use Windows 2012 or greater.
Microsoft Windows 2008 R2 DC STIG Benchmark, Version 1, Release 33
Rebundled benchmark to accommodate updated Rule ID.
Microsoft Windows 2008 R2 MS STIG, Version 1, Release 31
V-1073 - Updated requirement to note that support for the OS has ended and systems must use Windows 2012 or greater.
Microsoft Windows 2008 R2 MS STIG Benchmark, Version 1, Release 34
Rebundled benchmark to accommodate updated Rule ID.
Microsoft Windows 2008 Server DNS STIG, Version 1, Release 8
V-1073 - Added CAT I requirement to note that support for the OS has ended and systems must use Windows 2012 or greater.
Network Layer 2 Switch STIG - Ver 8, Rel 27
Sunset; no change to STIG
Network Other Devices STIG - Ver 8, Rel 23
Sunset; no change to STIG

APPLICABILITY GUIDE

Network Router Switch STIGs Applicability Guide
Indicates STIG/SRG to be used in place of legacy Network STIGs.

JANUARY 2020 MAINTENANCE RELEASE: JANUARY 24, 2020

JANUARY 2020 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Release Date: January 24, 2020

AAA Services SRG, Version 1, Release 2

V-80871

V-80871 - Requirement modified to replace SCA with SA in 4 places in the text.

Apache Server 2.4 UNIX Server STIG, Version 1, Release 3

V-92599

V-92599 - Modified verbiage to allow for vendor specific conf files, conf file locations and conf file content for determining validation of required modules.

V-92607

V-92607 - Clarified check to emphasize that the customlog directive is the important part of the check.

V-92609

V-92609 - Modified verbiage to allow for additional variables resulting in the same collection of data in log files.

V-92621

V-92621 - Added verbiage to allow the IP address of proxy providing originating IP address is also present in log files.

V-92629

V-92629 - Modified verbiage to allow for additional variables resulting in the same collection of data in log files.

V-92643

V-92643 - Clarified check criteria for consistency with intent of requirement.

V-92679

V-92679 - Modified check criteria to validate for headers_module (shared) instead of mod_headers.

V-92689

V-92689 - Modified verbiage to allow for vendor specific conf files and conf file locations for determining validation of required modules.

V-92759

V-92759 - Clarified check and fix criteria for consistency with intent of requirement.

Apache Server 2.4 Windows Server STIG, Version 1, Release 3

V-92405

V-92405 - Modified check criteria to restrict the SessionMaxAge to "no more than 600".

V-92433

V-92433 - Modified check criteria to reflect that the SessionMaxAge must be "at least 1" or greater to reflect the spirit of being explicitly configured and not relying on default.

V-92435

V-92435 - Modified check criteria to be consistent with similar check for mod_reqtimeout in the Apache Windows Site STIG ID V-92561.

Apache Server 2.4 Windows Site STIG, Version 1, Release 3

V-92511

V-92511 - Modified check criteria to correct directives for Apache 2.4 version. Existing verbiage was only valid in Apache 2.2.

V-92561

V-92561 - Modified check criteria to be consistent with similar check for mod_reqtimeout in the Apache Windows Server STIG ID V-92435.

Apple OS X 10.12 STIG, Version 1, Release 6

V-99043

V-99043 - Added new requirement that the use of this product is no longer supported by the vendor (Sunset STIG).

Apple OS X 10.13 STIG, Version 1, Release 4

V-81537

V-81537 - Switched to using "timed" instead of "ntpd".

Apple OS X 10.14 STIG, Version 1, Release 2

V-95799

V-95799 - Corrected typo in vulnerability discussion.

V-95815

V-95815 - Added the missing word "be" to the Check instructions regarding the array.

V-95887

V-95887 - Corrected typo in finding statement of the Check instructions.

V-95889

V-95889 - Corrected typo in finding statement of the Check instructions.

V-95903

V-95903 - Combined requirement with AOSX-14-002032.
V-95903 - Removed requirement.

V-95909

V-95909 - Updated Fix to reference the correct configuration profile.

V-95917

V-95917 - Updated text to account for pieces of AOSX-14-002018 and corrected a typo in Check instructions.

V-95927

V-95927 - Made the requirement and supporting text consistent to "tftpd" in all cases.

V-95943

V-95943 - Corrected single quote character in the command in Check instructions and the referenced policy in the Fix instructions.

BIND 9.x STIG, Version 1, Release 8

V-72365

V-72365 - Modified requirement to allow for latest supported version of BIND when BIND is installed as part of a specific vendor implementation where the vendor maintains the BIND patches.

V-72453

V-72453 - Modified requirement to add ECDSAP256SHA256 to allowed algorithms.

V-72469

V-72469 - Modified requirement to add ECDSAP256SHA256 to allowed algorithms.

V-72471

V-72471 - Added verbiage about DNSSEC awareness when forwarding all queries to ERS.
V-72471 - Modified requirement to add ECDSAP256SHA256 to allowed algorithms.

V-72495

V-72495 - Modified requirement to add ECDSAP256SHA256 to allowed algorithms.

V-72497

V-72497 - Modified requirement to add ECDSAP256SHA256 to allowed algorithms.

BlackBerry OS 10.3x STIG, Version 1, Release 4

V-98919

V-98919 - Added new requirement to sunset STIG.

Canonical Ubuntu 16.04 STIG, Version 1, Release 3

V-75471

V-75471 - Updated the finding statement.

V-75479

V-75479 - Updated the Rule Title to better reflect the requirement. Updated the check to look for all instances of "nullok". Updated the fix to reference all instances of "nullok".

V-75495

V-75495 - Updated the check command to also look in the systemd directory and uncommented configuration lines. Updated the finding statement to support the check command.

V-75505

V-75505 - Corrected a typo in the fix text to read "set superusers".

V-75507

V-75507 - Corrected a typo in the check and fix text that listed an incorrect file path for grub.cfg.

V-75523

V-75523 - Corrected a file path typo to read "/etc/default/aide" in the check and fix.

V-75541

V-75541 - Removed references to graphical user interfaces from the requirement.

V-75583

V-75583 - Removed the requirement because it is a duplicate of V-75513.

V-75635

V-75635 - Updated the CCI and list of satisfied SRG requirements.

V-75691

V-75691 - Removed the "arch=" configuration from the audit rule.

V-75693

V-75693 - Removed the "arch=" configuration from the audit rule.

V-75695

V-75695 - Added the "mount" command as an audit rule to the requirement.

V-75697

V-75697 - Removed the "arch=" configuration from the audit rule.

V-75699

V-75699 - Removed the "arch=" configuration from the audit rule.

V-75707

V-75707 - Removed the "arch=" configuration from the audit rule.

V-75709

V-75709 - Removed the requirement because it is a symlink to V-75715.

V-75711

V-75711 - Removed the requirement because it is a symlink to V-75715.

V-75713

V-75713 - Removed the requirement because it is a symlink to V-75715.

V-75755

V-75755 - Removed the "arch=" configuration from the audit rule.

V-75757

V-75757 - Removed the requirement because it is a symlink to V-75755.

V-75759

V-75759 - Removed the "arch=" configuration from the audit rule.

V-75761

V-75761 - Removed the "arch=" configuration from the audit rule.

V-75765

V-75765 - Removed the "arch=" configuration from the audit rule.

V-75767

V-75767 - Removed the "arch=" configuration from the audit rule.

V-75769

V-75769 - Removed the "arch=" configuration from the audit rule.

V-75777

V-75777 - Removed the "arch=" configuration from the audit rule.

V-75781

V-75781 - Removed the "arch=" configuration from the audit rule.

V-75783

V-75783 - Removed the "arch=" configuration from the audit rule.

V-75785

V-75785 - Removed the "arch=" configuration from the audit rule.

V-75787

V-75787 - Removed the "arch=" configuration from the audit rule.

V-75789

V-75789 - Removed the "arch=" configuration from the audit rule.

V-75797

V-75797 - Updated the Rule Title.

V-75825

V-75825 - Removed the "=" sign from the banner config to be consistent with other STIGs.

V-75833

V-75833 - Removed the "PermitUserEnvironment" from this requirement and added it as a standalone requirement.

V-75895

V-75895 - Updated the requirement to identify any ftpd package that might be installed.

V-75897

V-75897 - Updated the requirement to identify any tftpd package that might be installed.

V-80957

V-80957 - Updated the requirement to use "graphical user interface" in place of GUI. Added a note to the fix text.

V-80963

V-80963 - Merged the requirement with V-75635.

V-80969

V-80969 - Removed the "arch=" configuration from the audit rule.

V-98989

V-98989 - Added new requirement for the configuration of "PermitUserEnvironment".

V-99009

Added a requirement that the "pam_pwquality" module is installed and configured.

Cisco IOS Router NDM STIG, Version 1, Release 2

V-96037

V-96037 - Removed CISC-ND-000230.

V-96101

V-96101 - Removed CISC-ND-000840.

V-96177

V-96177 - Corrected rule title.

V-96181

V-96181 - Extended fix content.

Cisco IOS Router RTR STIG, Version 1, Release 2

V-96505

V-96505 - Corrected typo in check content.

V-96525

V-96525 - Corrected typo in check content.

V-96547

V-96547 - Corrected check and fix content.

V-96549

V-96549 - Corrected fix content.

V-96595

V-96595 - Corrected typo in check content.

V-96597

V-96597 - Corrected typo in check and fix content.

V-96611

V-96611 - Corrected typo in check and fix content.

Cisco IOS-XE Router NDM STIG, Version 1, Release 2

V-96219

V-96219 - Removed CISC-ND-000230.

V-96283

V-96283 - Removed CISC-ND-000840.

V-96359

V-96359 - Corrected rule title.

V-96363

V-96363 - Extended fix content.

Cisco IOS-XE Router RTR STIG, Version 1, Release 2

V-96857

V-96857 - Corrected typo in check content.

V-96877

V-96877 - Corrected typo in check content.

V-96899

V-96899 - Corrected check and fix content.

V-96901

V-96901 - Corrected fix content.

V-96947

V-96947 - Corrected typo in check content.

V-96949

V-96949 - Corrected typo in check and fix content.

V-96963

V-96963 - Corrected typo in check and fix content.

Cisco IOS-XR Router NDM STIG, Version 1, Release 2

V-96391

V-96391 - Removed CISC-ND-000230.

V-96433

V-96433 - Removed CISC-ND-000840.

V-96491

V-96491 - Corrected rule title.

Cisco IOS-XR Router RTR STIG, Version 1, Release 2

V-96695

V-96695 - Corrected typo in check content.

V-96713

V-96713 - Corrected check and fix content.

Citrix XenDesktop 7.x STIG, Version 1, Release 3

V-81415

V-81415 - Altered check/fix.

F5 BIG-IP Device Management 11.x STIG, Version 1, Release 7

V-60091

V-60091- Changed check and fix procedures to require a Set the MaxClients = 10 (or less) to fix the mismatch with the actual requirement.

Google Android 10.x STIG, Version 1, Release 2

V-98927

V-98927 - Corrected typo in check text.

V-98985

V-98985 - Revised Face authentication restriction: Face authentication may be used but must be configured to require open eyes.

(blank)

Updated STIG Overview and Configuration Table documents to remove restrictions on the use of Face authentication for the Pixel 4 phone.

Google Chrome for Windows STIG Benchmark, Version 1, Release 14

V-44757

Removed OVAL checking for disabled WebGL.

V-97525

Created OVAL for a new requirement, disable the development tools.

Google Chrome STIG, Version 1, Release 18

V-44757

V-44757 - Removed disable WebGL requirement.

V-79931

V-79931 - Added N/A for SIPRNet clause.

V-81591

V-81591 - Updated Active Directory verbiage.

V-81593

V-81593 - Updated Active Directory verbiage.

HBSS HIP 8 STIG, Version 4, Release 24

V-14532

V-14532 - Modified check content steps to validating correct policy.

V-14534

V-14534 - Modified verbiage of check content to be more consistent with the intent of the requirement.

V-14536

V-14536 - Modified check content steps to validating correct policy.

V-14537

V-14537 - Modified check content steps to validating correct policy.

V-14540

V-14540 - Modified check content steps to validating correct policy.

V-14541

V-14541 - Modified check content steps to validating correct policy.

V-14543

V-14543 - Modified check content steps to validating correct policy.

V-14544

V-14544 - Modified check content steps to validating correct policy.

V-14546

V-14546 - Modified check content steps to validating correct policy.

V-14547

V-14547 - Modified check content steps to validating correct policy.

V-14548

V-14548 - Modified check content steps to validating correct policy.

V-17893

V-17893 - Modified check content steps to validating correct policy.

V-31085

V-31085 - Modified check content steps to validating correct policy.

V-31086

V-31086 - Modified check content steps to validating correct policy.

HBSS Remote Console STIG, Version 4, Release 18

V-14513

V-14513 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-14514

V-14514 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-14515

V-14515 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-14516

V-14516 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-14517

V-14517 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-14518

V-14518 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-14571

V-14571 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

V-24014

V-24014 - Clarified all verbiage regarding requirement be N/A if using only a PKI web console access workstation.

Juniper Router NDM STIG, Version 1, Release 3

V-91111

V-91111 - Removed JUNI-ND-000230.

V-91143

V-91143 - Removed JUNI-ND-000830.

Layer 2 Switch SRG, Version 1, Release 5

V-62181

V-62181 - Remove rate limiting from DHCP snooping requirement.

V-62199

V-62199 - Removed SRG-NET-000512-L2S-000006.

Mainframe Product SRG, Version 1, Release 4

V-68145

V-68145 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68147

V-68147 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68149

V-68149 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68151

V-68151 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68153

V-68153 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68157

V-68157 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68189

V-68189 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

V-68265

V-68265 - Clarification on the use of SA and ISSO in the Mainframe Product SRG.

McAfee ENS 10-x STIG, Version 1, Release 6

V-79937

V-79937 - Added a note about Endpoint Security Firewall not required to be enforced as long as HIPS Firewall is enforced.

V-79939

V-79939 - Relaxed criteria to allow for a Standard Access, which allows users to run scans and update their signatures.

V-79949

V-79949 - Modified requirement to allow for local scan log files larger than 10MB, up to 100MB.

Microsoft Exchange 2013 Client Access Server STIG, Version 1, Release 3

V-69717

V-69717 - Corrected check criteria for import-module.

V-69775

V-69775 - Added additional criteria for applicability.

Microsoft Exchange 2013 Mailbox Server STIG, Version 1, Release 6

V-69975

V-69975 - Corrected registry key setting.

V-69977

V-69977 - Corrected registry key setting.

Microsoft Exchange 2013 Overview, N/A

N/A

Modified Overview document to remove reference requiring following the email policy STIG.

Microsoft Exchange 2016 Edge Transport Server STIG, Version 1, Release 4

V-80549

V-80549 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80551

V-80551 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80553

V-80553 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80555

V-80555 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80557

V-80557 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80559

V-80559 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80561

V-80561 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80565

V-80565 - Added a note for Not Applicable if using a third-party anti-spam product.

V-80585

V-80585 - Added a note for Not Applicable if using a third-party anti-spam product.

Microsoft IIS 7.0 Server STIG, Version 1, Release 19

V-99013

V-99013 - Added TBD to sunset STIG.

Microsoft IIS 7.0 Site STIG, Version 1, Release 19

V-99015

V-99015 - Added TBD to sunset STIG.

Microsoft Internet Explorer 10 STIG Benchmark, Version 1, Release 14

V-64727

Removed OVAL for requirement.

Microsoft Internet Explorer 10 STIG, Version 1, Release 16

V-64727

V-64727 - Added TBD CAT I for unsupported software.

Microsoft Internet Explorer 11 STIG Benchmark, Version 1, Release 14

V-97527

Added OVAL content for the "Internet Explorer Development Tools" requirement to the benchmark.

Microsoft SQL Server 2016 Database STIG, Version 1, Release 5

V-79067

V-79067 - Corrected ObjectCategory check.

V-79085

V-79085 - Updated zero value return and check for encrypted by password.

Microsoft SQL Server 2016 Instance STIG, Version 1, Release 8

V-79129

V-79129 - Updated check for the NT AUTHORITY SYSTEM account.

V-79179

V-79179 - Updated CLR Code logic.

V-79191

V-79191 - Changed password inheritance phrasing.

V-79211

V-79211 - Updated finding statement logic.

V-79293

V-79293 - Corrected script for audit check.

V-79295

V-79295 - Corrected script for audit check.

Microsoft Windows 2008 Server DNS STIG, Version 1, Release 7

V-58593

V-58593 - Corrected nslookup command syntax.

Microsoft Windows 2012 Server DNS STIG, Version 1, Release 13

V-58551

V-58551 - Modified fix criteria for correct syntax for expected outcome.

V-58573

V-58573 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58577

V-58577 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58579

V-58579 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58581

V-58581 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58593

V-58593 - Corrected nslookup command syntax.

V-58593 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58595

V-58595 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58605

V-58605 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58607

V-58607 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58617

V-58617 - Clarified check criteria regarding IAVMs.

V-58617 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58627

V-58627 - Added registry key alternative Fix.

V-58633

V-58633 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58641

V-58641 - Modified check criteria to allow for a N/A finding if Crypto folder does not exist.

V-58643

V-58643 - Modified check criteria to allow for a N/A finding if Crypto folder does not exist.

V-58645

V-58645 - Modified check criteria to allow for a N/A finding if Crypto folder does not exist.

V-58695

V-58695 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58711

V-58711 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58713

V-58713 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

V-58717

V-58717 - Corrected all requirement verbiage to read "Windows DNS Server" instead of "Windows 2008 DNS Server".

Microsoft Windows Defender Antivirus STIG Benchmark, Version 1, Release 5

N/A

Updated CPE-OVAL to make benchmark applicable to Windows Server 2019.

Microsoft Windows Defender Antivirus STIG, Version 1, Release 7

N/A

Modified Overview to include Windows Server 2019 as being subject to the Windows Defender STIG inspection.

V-75153

V-75153 - Corrected rule title and check content to reflect original requirement of joining Microsoft MAPs.

V-75167

V-75167 - Corrected rule title and check content to reflect original requirement of joining Microsoft MAPs.

Microsoft Windows Server 2012 and 2012 R2 DC STIG, Version 2, Release 19

V-91777

V-91777 - Change in discussion: The password must be changed twice to effectively remove the password history. "Changing once, waiting for replication to complete and the amount of time equal to or greater than the maximum Kerberos ticket lifetime, and changing again reduces the risk of issues."

Microsoft Windows Server 2012 and 2012 R2 MS STIG Benchmark, Version 2, Release 18

V-1115

Modified OVAL content to ignore the built-in domain administrator account assigned to local groups on a member server system.

V-1155

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-3449

Removed OVAL content from the benchmark in conjunction with the removal of the requirement from the STIG.

V-26483

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-26484

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-26485

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-26486

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

Microsoft Windows Server 2016 STIG Benchmark, Version 1, Release 12

V-73623

Modified OVAL content to ignore the built-in domain administrator account assigned to local groups on a member server system.

V-73759

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-73763

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-73767

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-73771

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-73775

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

Microsoft Windows Server 2016 STIG, Version 1, Release 10

V-91779

V-91779 - Change in discussion: The password must be changed twice to effectively remove the password history. "Changing once, waiting for replication to complete and the amount of time equal to or greater than the maximum Kerberos ticket lifetime, and changing again reduces the risk of issues."

Microsoft Windows Server 2019 STIG Benchmark, Version 1, Release 2

V-92965

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-93009

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-93011

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-93013

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-93015

Modified OVAL content to correct issue where the Domain Admins group was not detected as being assigned the user right on a member server.

V-93281

Modified OVAL content to ignore the built-in domain administrator account assigned to local groups on a member server system.

Microsoft Windows Server 2019 STIG, Version 1, Release 3

V-93211

V-93211 - Change in discussion: The password must be changed twice to effectively remove the password history. "Changing once, waiting for replication to complete and the amount of time equal to or greater than the maximum Kerberos ticket lifetime, and changing again reduces the risk of issues."

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

V-79053

Updated OVAL to verify "security.tls.version.max" is set to 4.
Removed deprecated sub-requirements from OVAL.

Mozilla Firefox STIG, Version 4, Release 28

V-15983

V-15983 - Updated to include TLS 1.3.

V-79053

V-79053 - Removed deprecated requirements.

Mozilla Firefox Windows STIG Benchmark, Version 1, Release 5

V-79053

Removed OVAL for deprecated requirement to disable background submittion of information to Mozilla.
Removed deprecated sub-requirements from OVAL.

Network Device Management SRG, Version 3, Release 2

V-55037

V-55037 - Removed SRG-APP-000023-NDM-000205.

V-55039

V-55039 - Removed SRG-APP-000024-NDM-000206.

V-55041

V-55041 - Removed SRG-APP-000025-NDM-000207.

V-55061

V-55061 - Removed SRG-APP-000075-NDM-000217.

V-55063

V-55063 - Removed SRG-APP-000076-NDM-000218.

V-55065

V-55065 - Removed SRG-APP-000079-NDM-000219.

V-55069

V-55069 - Removed SRG-APP-000345-NDM-000290.

V-55071

V-55071 - Removed SRG-APP-000346-NDM-000291.

V-55077

V-55077 - Removed SRG-APP-000359-NDM-000294.

V-55103

V-55103 - Removed SRG-APP-000148-NDM-000246.

V-55105

V-55105 - Removed SRG-APP-000149-NDM-000247.

V-55107

V-55107 - Removed SRG-APP-000151-NDM-000248.

V-55113

V-55113 - Removed SRG-APP-000163-NDM-000251.

V-55117

V-55117 - Removed SRG-APP-000165-NDM-000253.

V-55135

V-55135 - Removed SRG-APP-000173-NDM-000260.

V-55139

V-55139 - Removed SRG-APP-000174-NDM-000261.

V-55141

V-55141 - Removed SRG-APP-000175-NDM-000262.

V-55145

V-55145 - Removed SRG-APP-000177-NDM-000263.

V-55151

V-55151 - Removed SRG-APP-000108-NDM-000232.

V-55175

V-55175 - Removed SRG-APP-000234-NDM-000272.

V-55181

V-55181 - Removed SRG-APP-000268-NDM-000274.

V-55185

V-55185 - Removed SRG-APP-000291-NDM-000275.

V-55187

V-55187 - Removed SRG-APP-000292-NDM-000276.

V-55189

V-55189 - Removed SRG-APP-000293-NDM-000277.

V-55193

V-55193 - Removed SRG-APP-000294-NDM-000278.

V-55207

V-55207 - Removed SRG-APP-000320-NDM-000284.

V-55211

V-55211 - Removed SRG-APP-000325-NDM-000285.

V-55213
V-55213 - Removed SRG-APP-000126-NDM-000242.

V-55237
V-55237 - Removed SRG-APP-000377-NDM-000301.

V-55247
V-55247 - Removed SRG-APP-000389-NDM-000306.

V-55251
V-55251 - Removed SRG-APP-000391-NDM-000308.

V-55253
V-55253 - Removed SRG-APP-000392-NDM-000309.

V-55257
V-55257 - Removed SRG-APP-000396-NDM-000311.

V-55259
V-55259 - Removed SRG-APP-000397-NDM-000312.

V-55291
V-55291 - Removed SRG-APP-000516-NDM-000332.

V-55293
V-55293 - Removed SRG-APP-000516-NDM-000333.

V-55299
V-55299 - Revised rule title and changed to Cat 1.

V-55301
V-55301 - Removed SRG-APP-000516-NDM-000337.

V-55303
V-55303 - Removed SRG-APP-000516-NDM-000338.

V-55305
V-55305 - Removed SRG-APP-000516-NDM-000339.

V-55311
V-55311 - Removed SRG-APP-000516-NDM-000342.

V-80967
V-80967 - Removed SRG-APP-000175-NDM-000350.

V-99017
V-99017 - Add requirement to send log data to a syslog server.

V-99019

V-99019 - Add requirement that OS must be supported by the vendor.

Network Infrastructure Policy STIG, Version 9, Release 10

V-66359

V-66359 - Removed NET2003.

Oracle 11.2g Database STIG, Version 1, Release 17

V-52255

V-52255 - Updated TLS version to 1.2.

V-52257

V-52257 - Updated TLS version to 1.2.

V-52259

V-52259 - Updated TLS version to 1.2.

V-52285

V-52285 - Updated TLS version to 1.2.

V-52289

V-52289 - Updated TLS version to 1.2.

V-52293

V-52293 - Updated TLS version to 1.2.

V-52295

V-52295 - Updated TLS version to 1.2.

V-52331

V-52331 - Updated TLS version to 1.2.

V-52345

V-52345 - Removed fix text content in check text.

V-52351

V-52351 - Removed fix text content in check text.

V-52397

V-52397 - Updated TLS version to 1.2.

V-75031

V-75031 - Updated TLS version to 1.2.

Oracle Database 12c STIG, Version 1, Release 16

V-61433

V-61433 - Updated administrative accounts list.

V-61437

V-61437 - Updated administrative accounts list.

V-61439

V-61439 - Updated administrative accounts list.

V-61543

V-61543 - Updated TLS version to 1.2.

V-61703

V-61703 - Updated TLS version to 1.2.

V-61705

V-61705 - Updated TLS version to 1.2.

V-61707

V-61707 - Updated TLS version to 1.2.

V-61709

V-61709 - Updated TLS version to 1.2.

V-61733

V-61733 - Updated TLS version to 1.2.

V-61737

V-61737 - Updated TLS version to 1.2.

V-61741

V-61741 - Updated TLS version to 1.2.

V-61743

V-61743 - Updated TLS version to 1.2.

V-61815

V-61815 - Removed duplicate tcp valid node checking.

V-61845

V-61845 - Updated TLS version to 1.2.

Oracle HTTP Server 12.1.3 STIG, Version 1, Release 6

V-64137

V-64137 - Update TLS and .conf file info.

V-64139

V-64139 - Update TLS and .conf file info.

V-64145

V-64145 - Update TLS and .conf file info.

V-64411

V-64411 - Update TLS and .conf file info.

V-64419

V-64419 - Update TLS and .conf file info.

V-64435

V-64435 - Update TLS and .conf file info.

V-64443

V-64443 - Update TLS and .conf file info.

V-64513

V-64513 - Update TLS and .conf file info.

V-64521

V-64521 - Update TLS and .conf file info.

V-64545

V-64545 - Update TLS and .conf file info.

V-64561

V-64561 - Update TLS and .conf file info.

V-64569

V-64569 - Update TLS and .conf file info.

V-64583

V-64583 - Update TLS and .conf file info.

V-64701

V-64701 - Update TLS and .conf file info.

Palo Alto Networks Application Layer Gateway (ALG) STIG, Version 1, Release 5

V-62579

V-62579 - Use either Drop or reset-both.

V-62581

V-62581 - Use either Drop or reset-both.

Palo Alto Networks IDPS STIG, Version 1, Release 4

V-62647

V-62647 - Use either Drop or reset-both.

V-62651

V-62651 - Change the wording to allow the info level to be omitted when packet captures are needed if that information is not needed since in my option that does not rise to the level of CAT III.

V-62661

V-62661 - Use either Drop or reset-both.

Palo Alto Networks Network Device Management (NDM) STIG, Version 1, Release 4

V-62765

V-62765 - The NDM is incorrect. According to the NIST eval, if the Palo Alto is in Common Criteria mode (configured to use NIST FIPS 140-2 modules for cryptographic functions, then it will use HTTP OCSP with TLS.

Red Hat 6 STIG Benchmark, Version 1, Release 26

V-38675

Updated the OVAL to ensure the limit is a non-negative integer.

V-38684

Updated the OVAL to ensure the limit is a non-negative integer.

Red Hat Enterprise Linux 7 STIG Benchmark, Version 2, Release 6

V-72217

Updated the OVAL to ensure the limit is a non-negative integer.

Red Hat Enterprise Linux 7 STIG, Version 2, Release 6

V-71855

V-71855 - Updated the CCI for this requirement.

V-72269

V-72269 - Added "chrony" as a vaild application that will satisfy the requirement.

Solaris 10 SPARC STIG, Version 1, Release 26

V-792

V-792 - Updated the permissions for man page files.

Solaris 10 X86 STIG, Version 1, Release 26

V-792

V-792 - Updated the permissions for man page files.

Solaris 11 SPARC STIG Benchmark, Version 1, Release 14

V-47893

Removed OVAL for Solaris IPS requirement.

V-47901

Removed OVAL for Solaris IPS requirement.

V-47905

Removed OVAL for Solaris IPS requirement.

V-47909

Removed OVAL for Solaris IPS requirement.

V-47913

Removed OVAL for Solaris IPS requirement.

V-47917

Removed OVAL for Solaris IPS requirement.

V-47921

Removed OVAL for Solaris IPS requirement.

V-48077

Updated the OVAL to use the correct allowed user lists.

Solaris 11 SPARC STIG, Version 1, Release 20

V-47947

V-47947 - Removed HBSS client requirement due to lack of commercial supported client availability.

V-48099

V-48099 - Changed the grep command in the Check.

Solaris 11 X86 STIG Benchmark, Version 1, Release 14

V-47893

Removed OVAL for Solaris IPS requirement.

V-47901

Removed OVAL for Solaris IPS requirement.

V-47905

Removed OVAL for Solaris IPS requirement.

V-47909

Removed OVAL for Solaris IPS requirement.

V-47913

Removed OVAL for Solaris IPS requirement.

V-47917

Removed OVAL for Solaris IPS requirement.

V-47921

Removed OVAL for Solaris IPS requirement.

V-48077

Updated the OVAL to use the correct allowed user lists.

Solaris 11 X86 STIG, Version 1, Release 20

V-47947

V-47947 - Removed HBSS client requirement due to lack of commercial supported client availability.

V-48099

V-48099 - Changed the grep command in the Check.

SUSE Linux Enterprise Server 12 STIG, Version 1, Release 4

V-77051

V-77051 - Updated the requirement to use /etc/issue.

V-77069

V-77069 - Updated the requirement to utilize the systemd file structure.

V-77089

V-77089 - Combined this requirement with V-77105.

V-77105

V-77105 - Combined V-77089 with this requirement.

V-77117

V-77117 - Updated the check command to properly identify misconfigured accounts.

V-77123

V-77123 - Updated the requirement to also include the "retry" value.

V-77131

V-77131 - Updated the requirement to allow for a delay greater than or equal to 4 seconds.

V-77143

V-77143 - Modified the requirement so that "root" was not the primary account referenced.

V-77145

V-77145 - Modified the requirement so that "root" was not the primary account referenced.

V-77149

V-77149 - Added a note to the requirement that each locally defined partition should be checked.

V-77151

V-77151 - Updated the check and fix to better address the actual OS configuration.

V-77153

V-77153 - Updated the check and fix to better address the actual OS configuration.

V-77155

V-77155 - Corrected a typo where "xattr" was referenceds in the requirement.

V-77171

V-77171 - Updated the requirement to focus on CLI only.

V-77253

V-77253 - Added a note to the requirement that each locally defined partition should be checked.

V-77307

V-77307 - Updated the Rule Title.

V-77327

V-77327 - Updated the check command to use "grep -iw".

V-77329

V-77329 - Removed the requirement because it is a symlink to "sudo".

V-77333

V-77333 - Corrected a typo in the audit rules.

V-77335

V-77335 - Corrected a typo in the audit rules.

V-77343

V-77343 - Removed the requirement because it is a symlink to "kmod".

V-77345

V-77345 - Removed the requirement because it is a symlink to "kmod".

V-77439

V-77439 - Combined V-77445 with this requirement.

V-77443

V-77443 - Added "INFO" as a vaild configuration option.

V-77445

V-77445 - Combined this requirement with V-77439.

V-77451

V-77451 - Removed the "PermitUserEnvironment" from this requirement and added it as a standalone requirement.

V-77469

V-77469 - Added "sandbox" as a valid configuration option.

V-77471

V-77471 - Removed "delayed" as a vaild configuration option.

V-77509

V-77509 - Updated a typo in the finding statement.

V-81709

V-81709 - Updated the requirement to use the "pam_tally2" module.

V-98987

V-98987 - Added a new requirement for CTRL-ALT-DEL disablement in a Graphical User Interface.

V-99011

V-99011 - Added a new requirement to check for "PermitUserEnvironment".

Symantec ProxySG ALG STIG, Version 1, Release 2

V-94225

V-94225 - Changed the check and fix to clarify that HSM is not a requirement.

Symantec ProxySG NDM STIG, Version 1, Release 2

V-94413

V-94413 - Changed the check and fix to not require traffic limits.

VMware vSphere 6.5 ESXi STIG, Version 1, Release 3

V-94023

V-94023 - Added N/A statement when host profiles are not used to join AD.

V-94349

V-94349 - Modified check/fix.

V-94505

V-94505 - Added N/A statement when host profiles are not used to join AD.

V-94507

V-94507 - Added N/A statement when host profiles are not used to join AD.

V-94529

V-94529 - Added N/A statement when host profiles are not used to join AD.

V-94531

V-94531 - Added N/A statement when host profiles are not used to join AD.

V-94543

V-94543 - Added N/A statement when host profiles are not used to join AD.

V-94545

V-94545 - Added N/A statement when host profiles are not used to join AD.

VMware vSphere 6.5 vCenter Server for Windows STIG, Version 1, Release 3

V-94775

V-94775 - Adjusted permissions.

V-94801

V-94801 - Modified syntax.

z/OS PDI list spreadsheet, Version 6, Release 43

V-3229

New automation

V-3230

New automation

V-7558

New automation

z/OS SRR Scripts, Version 6, Release 43

V-3229

New automation

V-3230

New automation

V-7558

New automation

N/A

Changed scripts to continue processing when user running scripts does not have a HOME directory. Changed scripts to reduce the amount of information collected for ACF2 and to continue processing when user running scripts has a HOME of Root (/).