OCTOBER 2019 Maintenance Release: STIGS to Be Released

Release Date: Oct 25 2019

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

V-92607

Added note regarding /etc/httpd/logs as sometimes being a capital "L".

Apache Server 2.4 Windows Server STIG, Version 1, Release 2

V-92337

Corrected check verbiage to Windows platform.

Application Security and Development STIG, Version 4, Release 10

V-69501

Updated the check language to specify if value is NOT checked it’s a finding.

Application Server SRG, Version 2, Release 7

V-35217

Added clarity to discussion, check and fix regarding hashing of log files

V-35306

Removed requirement

V-35381

Added clarity to mutual authentication requirement

Arista MLS DCS-7000 Series NDM STIG, Version 1, Release 3

V-60885

Corrected authorization command in the check and fix content.

Database SRG, Version 2, Release 9

V-32366

V-32366 Removed user session auditing

EDB Postgres Advanced Server STIG, Version 1, Release 6

V-68893

V-68893 Removed user session auditing

F5 BIG-IP Device Management 11.x STIG, Version 1, Release 6

V-97729

Added new requirement

N/A

Update to Overview for clarification

F5 BIG-IP Local Traffic Manager 11.x STIG, Version 1, Release 3

V-60311

Set a TCP profile 'idle-timeout' set to 600/900 seconds would be more accurate to meet the requirement.

Google Chrome Browser STIG, Version 1, Release 17

V-44805
Updated CCIs in V-81583, V-44805, V-52795.

V-52795
Updated CCIs in V-81583, V-44805, V-52795.

V-81583
Updated CCIs in V-81583, V-44805, V-52795.

V-97525
Added "V-97525" to disable developer mode.

Google Chrome for Windows STIG Benchmark, Version 1, Release 13

V-44805
Disabled OVAL to check Chrome version.

HBSS ePO 5.3/5.9x STIG, Version 1, Release 19

V-14489
Clarified ports in check verbiage.

V-14495
Check verbiage modified to remove reference to deny-by-default"
Modified STIG ID to reflect ePO 5.10

V-14510
Added epo_HBSSEPO_Events DB to allowed SQL databases as added in ePO 5.10.
Modified STIG ID to reflect ePO 5.10

V-14579
Clarified steps to conduct the check validation.
Modified STIG ID to reflect ePO 5.10

V-14868
Added note for ePO 5.10 that due to the password complexity when not using PKI, this check is N/A.
Modified STIG ID to reflect ePO 5.10

V-15358
Corrected URL references in check verbiage.
Modified STIG ID to reflect ePO 5.10

V-17897
Added verbiage about not selecting the ePO events DB when validating.
Modified STIG ID to reflect ePO 5.10

V-24013

Added verbiage about not selecting the ePO events DB when validating.
Modified STIG ID to reflect ePO 5.10

V-24021
Modified referenced URL for PKI/PKE information.
Modified STIG ID to reflect ePO 5.10

V-24022
Modified referenced URL for PKI/PKE information.
Modified STIG ID to reflect ePO 5.10

V-24023
Modified referenced URL for PKI/PKE information.
Modified STIG ID to reflect ePO 5.10

V-47161
Modified referenced URL for Enhanced Reporting documentation.
Modified STIG ID to reflect ePO 5.10

V-97533
Added new CAT 1 to reflect that ePO 5.3 and prior versions are unsupported versions.

N/A
Renamed HBSS ePO 5.3/5.9 STIG to HBSS ePO 5x

HBSS HIP 8 Firewall STIG, Version 1, Release 14

V-47483
Clarified requirement verbiage for intent.

V-47487
Correction to domain directive when configuring CAG.

HBSS McAfee Agent STIG, Version 4, Release 19

V-14521
Updated fix verbiage to be consistent with check.

HP FlexFabric Switch NDM STIG, Version 1, Release 2

V-66241
Correct check content.

IBM DB2 V10.5 LUW STIG, Version 1, Release 4

V-74661
V-74661 Removed user session auditing

Infoblox 7.x DNS STIG, Version 1, Release 8

V-68519

Corrected check verbiage from "Zone Transfers" tab to "Updates" tab.

Intrusion Detection and Prevention System Technology SRG, Version 2, Release 5

V-55331
Changed SCA to individual designated ty the SCA (SA recommended)

V-55363
Changed SCA to individual designated ty the SCA (SA recommended)

V-55379
Changed SCA to individual designated ty the SCA (SA recommended)

V-55385
Removed reference to SCA and replace with SA at a minimum

V-55387
Changed SCA to individual designated ty the SCA (SA recommended)

V-55389
Changed SCA to individual designated ty the SCA (SA recommended)

V-55391
Changed SCA to individual designated ty the SCA (SA recommended)

V-55393
Changed SCA to individual designated ty the SCA (SA recommended)

V-55597
Changed SCA to system administrator

Juniper Router RTR STIG, Version 1, Release 3

V-90897
Add clarification to check content.

V-90905
Add clarification to check content.

V-96005
Add clarification to check content.

Mainframe Product SRG, Version 1, Release 3

V-68245
correct typo: change 'where' to 'when'.

McAfee ENS 10-x STIG, Version 1, Release 5

V-80045
Added note regarding HIPS signature 3910 to be consistent with VSE 8.8 STIG.

McAfee VirusScan 8.8 Local Client STIG Benchmark, Version 1, Release 2

V-6599

Disabled the OVAL because the correct logic is impossible to do with OVAL and the current way McAfee stores and maintains the values that need to be checked.

V-6600

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6601

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6602

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6604

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6611

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6612

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6614

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6615

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6616

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6617

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6618

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6620

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6625

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-6627

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-14654

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-42565

Disabled the OVAL because the correct logic is impossible to do with OVAL and the current way McAfee stores and maintains the values that need to be checked.

V-42566

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

V-42567

Updated OVAL to correctly identify a weekly scan instead of assuming the weekly scan is using the pre-existing Full Scan job that was created when Virus Scanner was installed.

McAfee VirusScan 8.8 Managed Client STIG Benchmark, Version 1, Release 3

V-6585

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6599

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6600

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6601

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6602

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6604

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6611

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6612

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6614

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6615

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6616

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6617

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6618

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6620

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6625

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-6627

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-14654

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-42532

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-42533

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

V-42534

Disabled the OVAL because McAfee is storing information required for the check in an encrypted database that the OVAL cannot access.

McAfee VirusScan 8.8 Managed Client STIG, Version 5, Release 21

V-42531

Clarified verbiage regarding approval authority for justified exclusions.

McAfee VSEL 1.9/2.0 Local Client STIG, Version 1, Release 5

V-63133

Updated check verbiage with correct command line criteria.

Microsoft .Net Framework STIG 4.0 STIG, Version 1, Release 9

V-7055

Added clarity to finding statement

Microsoft Exchange 2013 Mailbox Server STIG, Version 1, Release 5

V-69955

Corrected Fix text to read $False.

V-70043

Clarified verbiage for allowed domains when Auto Forwarding.

Microsoft Exchange 2016 Mailbox Server STIG, Version 1, Release 4

V-80637

Corrected Fix text to read $False.

V-80707

Clarified verbiage for allowed domains when Auto Forwarding.

Microsoft IIS 8.5 Server STIG, Version 1, Release 9

V-76689

Altered fix text in V-76689.

Microsoft IIS 8.5 Site STIG, Version 1, Release 9

V-76807

Altered V-76807 to not be a finding if port 80 is not used.

V-76839

Altered V-76839 such that a value of zero is also a finding.

V-76859

Added NA for public site in V-76859.

V-76861

Altered fix text in V-76861.
Added NA for public site in V-76861.

Microsoft Office System 2013 STIG, Version 1, Release 9

V-17547

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17560

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17581

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17583

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17590

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17605

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17612

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17617

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17619

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17627

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17659
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17660
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17661
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17664
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17669
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17670
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17731
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17740
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17741
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17749
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17750
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17759
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17765
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17768
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17769
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17773
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-17805
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-26630
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-26704
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40860
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40861
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40862
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40863
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40864
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40875
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40879
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40880
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40881
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40882
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40883
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40884
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40885

Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40886
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

V-40887
Corrected finding statements to remove "for every user profile hive" since check only validates the HKCU.

N/A
Repackaged without duplicated V-17547

Microsoft SharePoint 2013 STIG, Version 1, Release 8

V-59965
Updated SSL Cipher suite text order in V-59965, V-59967, V-59969, V-59971, V-59989,

V-59967
Updated SSL Cipher suite text order in V-59965, V-59967, V-59969, V-59971, V-59989,

V-59969
Updated SSL Cipher suite text order in V-59965, V-59967, V-59969, V-59971, V-59989,

V-59971
Updated SSL Cipher suite text order in V-59965, V-59967, V-59969, V-59971, V-59989,

V-59989
Updated SSL Cipher suite text order in V-59965, V-59967, V-59969, V-59971, V-59989,

V-60005
Updated V-60005 to state IIS_IUSRS instead of IIS_WPG

Microsoft SQL Server 2016 Instance STIG, Version 1, Release 7

V-79143
V-79143 Removed user session auditing

V-79149
V-79149 Changed check to account for Application Log or Security Log

V-79195
V-79195 Moved TLS 1.2 to a separate check

V-79239
V-79239 Added TRACE_CHANGE_GROUP to script

V-79259
V-79259 Added script to check audit settings

V-79261

V-79261 Added script to check audit settings

V-79263

V-79263 Added script to check audit settings

V-79265

V-79265 Added script to check audit settings

V-97521

V-97521 TLS 1.2 encryption added as a separate requirement

Microsoft Windows 10 STIG Benchmark, Version 1, Release 16

V-68819

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

Microsoft Windows Server 2016 STIG Benchmark, Version 1, Release 11

V-73247

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73299

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73301

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73443

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73445

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73461

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73477

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73591

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

V-73809

Removed the "OR" operators from the criteria elements in the OVAL, which could cause validation issues and errors with some SCAP tools.

Mozilla Firefox STIG Benchmark, Version 1, Release 4

V-17988

Disabled OVAL to check Firefox version.

Mozilla Firefox STIG, Version 4, Release 27

V-17988

Updated V-17988 to state any supported version, not strictly ESR.

V-64891

Modified VulDiscussion in V-64891.

V-97529

Added "V-97529" to disable developer mode.

MS Internet Explorer 11 STIG, Version 1, Release 18

V-97527

Added "V-97527" to disable developer mode.

Multifunction Device and Network Printers STIG, Version 2, Release 14

V-97711

MFD STIG requirement for USB and SIPR needed

Network Device Management SRG, Version 2, Release 15

V-55055

Add to the requirement to lock-out account for 15 minutes.

V-55081

NTP synchronization intervals are within seconds (64 to 10024)--not hours.

V-55083

No such thing in the RFC 1305 or 5905 to specify offset values as to when to synchronize.

V-55087

Removed requirement as there are no DoD list of auditable events.

V-55109

Correct rule title phrasing.

V-55153

Correct typo in check content.

V-55169
Removed requirement as all admins need to see log data.

V-55177
Operator class must be able to see error messages.

V-55195
Redundant with SRG-APP-000190-NDM-000267.

V-55231
Remove "different geographical regions" from rule title.

V-55255
Remove bidirectional and add FIPS-140-2 to rule title and check/fix content.

V-55267
Add FIPS-140-2 to rule title and check/fix content.

V-55269
Correct rule title phrasing.

V-55285
Redundant with SRG-APP-000026-NDM-000208, SRG-APP-000027-NDM-000209, SRG-APP-000028-NDM-000210, and SRG-APP-000029-NDM-000211.

V-55289
This is policy--not configurable.

V-55295
Change rule title from "generate audit log events" to "generate log records".

V-55299
Change rule title to The device must be configured to use an AAA server for authenticating users prior to granting administrative access.

V-55307
Change requirement to backup configuration after a change is made.

V-64001
Correct rule title phrasing and remove statement regarding setting the privilege level in the check content.

Network Infrastructure Policy STIG, Version 9, Release 9

V-14737
Correct CCI

Network WLAN AP-Enclave NIPRNet Role STIG, Version 6, Release 16

V-97417

Added new WIDS check to STIG (requirement had previously been in the Network Infrastructure Policy STIG).

Oracle 11.2g Database STIG, Version 1, Release 16

V-53981

V-53981 Added check for password file permissions.

Oracle Database 12c STIG, Version 1, Release 15

V-61431

V-61431 Added check for password file permissions

V-61459

V-61459 Updated default usernames in the script

V-61605

V-61605 Updated maximum failed login attempts to remove duplicate

V-61607

V-61607 Removed duplicate failed login attempts

V-61739

V-61739 Added approved by ISSO statement to check

Oracle Linux 6 STIG, Version 1, Release 17

V-97233

Added a requirement to implement DoD-approved encryption.

Palo Alto Networks IDPS STIG, Version 1, Release 3

V-62677

PANW-IP-000041 - In the fix text change to:
In the "Source" tab, for "Zone", select the "External zone, for Source Address", select "Any".
In the "Destination" tab, "Zone", select "Internal zone, for Destination Address", select "Any".

PostgreSQL 9.x STIG, Version 1, Release 6

V-73021

V-73021 Removed user session auditing

V-73071

V-73071 Changed specific RHEL reference to FIPS 140-2 certified

Red Hat 6 STIG Benchmark, Version 1, Release 25

V-38511

Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38523
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38524
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38526
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38528
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38529
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38532
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38533
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38535
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38537
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38539
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38542
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38544
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38548
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38600
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38601
Updated the OVAL to also check /etc/sysctl.d/*.conf.

V-38583
Updated OVAL to not check "/boot/efi/EFI/redhat/grub.conf".

Red Hat Enterprise Linux 6 STIG, Version 1, Release 24

V-38511
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38523
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38524
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38526
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38528
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38529
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38532
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38533
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38535
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38537
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38539
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38542
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38544
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38548
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38583

Removed " /boot/efi/EFI/redhat/grub.conf" from the requirement.

V-38596
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38597
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38600
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38601
Added the "/etc/sysctl.d/" directory and example output to the check and fix.

V-38609
Updated the requirements finding statement.

V-38617
Updated the check command to reduce false positives. Updated the cipher list in the fix text.

V-97229
Added a requirement to implement DoD-approved encryption.

V-97231
Added a requirement to validate and configure message authentication codes for use with ssh.

Red Hat Enterprise Linux 7 STIG Benchmark, Version 2, Release 5

V-71997
Updated OVAL to accept RHEL 7.7 as supported.

V-72067
Updated OVAL to decouple RHEL version check.

V-72221
Updated OVAL to decouple RHEL version check.

V-72253
Updated OVAL to decouple RHEL version check.

V-72433
Updated OVAL to handle quotes around oscp_on.

Red Hat Enterprise Linux 7 STIG, Version 2, Release 5

V-71899
Added a "Not Applicable" statement to the requirement.

V-71991

Updated the second set of commands in the check text.

V-71997
Added End of Life information for RHEL 7.7 to the check.

V-72227
Updated the check to look at "id_provider" in the /etc/sssd/sssd.conf file.

V-72229
Updated the check to look at "id_provider" in the /etc/sssd/sssd.conf file.

V-72231
Updated the check to look at "id_provider" in the /etc/sssd/sssd.conf file.

Red Hat JBoss Enterprise Application Platform (EAP) 6.3 STIG , Version 1, Release 4

V-62287
Corrected finding statement.

Riverbed SteelHead CX v8 NDM STIG, Version 1, Release 2

V-62847
Rewrite the check/fix to require using an SNMP trap or using a syslog/SIEM configuration to forward the notice.

Router SRG, Version 3, Release 4

V-78273
Add clarification to check content.

V-78281
Add clarification to check content.

V-92243
Add clarification to check content.

Samsung Android OS 7 with Knox 3.x STIG, Version 1, Release 6

V-76621
Changed password complexity rule for the device

V-76659
Changed password complexity rule for the Knox container

N/A
Updated Configuration Tables document to change password complexity rule for the device and Knox container

Samsung Android OS 8 with Knox 3.x COBO STIG, Version 1, Release 4

V-80201
Changed password complexity rule for the device

Samsung Android OS 8 with Knox 3.x COPE STIG, Version 1, Release 4

V-80323

Changed password complexity rule for the device

V-80325

Changed password complexity rule for the Knox container

Samsung Android OS 8 with Knox 3.x STIG, Version 1, Release 4

N/A

Updated Configuration Tables document to change password complexity rule for the device and Knox container

Samsung Android OS 9 Knox 3-x COBO KPE AE STIG, Version 1, Release 2

V-92933

Changed password complexity rule for the device

Samsung Android OS 9 Knox 3-x COBO KPE Legacy STIG, Version 1, Release 2

V-93639

Changed password complexity rule for the device

Samsung Android OS 9 Knox 3-x COPE KPE AE STIG, Version 1, Release 2

V-93841

Changed password complexity rule for the device

Samsung Android OS 9 Knox 3-x COPE KPE Legacy STIG, Version 1, Release 2

V-93939

Changed password complexity rule for the device

V-93945

Changed password complexity rule for the Knox container

Samsung Android OS 9 with Knox 3.x STIG, Version 1, Release 2

N/A

Updated Configuration Tables documents to change password complexity rule for the device and Knox container

Updated Supplemental document to clarify STIG requirements related to Common Criteria settings, Note 10 Legacy support, and Secure Startup implementation

Solaris 11 SPARC STIG Benchmark, Version 1, Release 13

V-47781

Updated OVAL checking global zone status.

V-47783

Updated OVAL checking global zone status.

V-47785

Updated OVAL checking global zone status.

V-47787
Updated OVAL checking global zone status.

V-47789
Updated OVAL checking global zone status.

V-47791
Updated OVAL checking global zone status.

V-47793
Updated OVAL checking global zone status.

V-47795
Updated OVAL checking global zone status.

V-47797
Updated OVAL checking global zone status.

V-47799
Updated OVAL checking global zone status.

V-47801
Updated OVAL checking global zone status.

V-47803
Updated OVAL checking global zone status.

V-47835
Updated OVAL checking global zone status.

V-47843
Updated OVAL checking global zone status.

V-47845
Updated OVAL checking global zone status.

V-47895
Updated OVAL checking global zone status.

V-47897
Updated OVAL to handle permissions and global zones better.
Disabled OVAL to check /etc/zones owner, group, and permissions.

V-47911
Updated OVAL to use packagecheck_test.
Disabled OVAL checking whether the FTP server is installed.

V-47915

Updated OVAL to use packagecheck_test.

Disabled OVAL checking whether the telnet server is installed.

V-47939

Updated OVAL checking global zone status.

V-48127

Updated OVAL checking global zone status.

Solaris 11 SPARC STIG, Version 1, Release 19

V-48047

Updated requirement to have a 5 second lock timeout.

V-48077

Added more users to the permitted list of accounts.

V-48099

Added a trailing space to the grep in the check command.

Solaris 11 X86 STIG Benchmark, Version 1, Release 13

V-47781

Updated OVAL checking global zone status.

V-47783

Updated OVAL checking global zone status.

V-47785

Updated OVAL checking global zone status.

V-47787

Updated OVAL checking global zone status.

V-47789

Updated OVAL checking global zone status.

V-47791

Updated OVAL checking global zone status.

V-47793

Updated OVAL checking global zone status.

V-47795

Updated OVAL checking global zone status.

V-47797

Updated OVAL checking global zone status.

V-47799
Updated OVAL checking global zone status.

V-47801
Updated OVAL checking global zone status.

V-47803
Updated OVAL checking global zone status.

V-47835
Updated OVAL checking global zone status.

V-47843
Updated OVAL checking global zone status.

V-47845
Updated OVAL checking global zone status.

V-47895
Updated OVAL checking global zone status.

V-47897
Updated OVAL to handle permissions and global zones better.
Disabled OVAL to check /etc/zones owner, group, and permissions.

V-47911
Updated OVAL to use packagecheck_test.
Disabled OVAL checking whether the FTP server is installed.

V-47915
Updated OVAL to use packagecheck_test.
Disabled OVAL checking whether the telnet server is installed.

V-47939
Updated OVAL checking global zone status.

V-48001
Updated OVAL checking global zone status.

V-48127
Updated OVAL checking global zone status.

Solaris 11 X86 STIG, Version 1, Release 19

V-48047
Updated requirement to have a 5 second lock timeout.

V-48077
Added more users to the permitted list of accounts.

V-48099
Added a trailing space to the grep in the check command.

SUSE Enterprise Linux 12 STIG, Version 1, Release 3

V-77045
Updated the check content with current version information

V-77053
Updated the requirement to use the correct banner path

V-77055
Updated the requirement to use the correct banner path

V-77059
Updated the rule title, check, and fix to reflect that 'vlock' is now a part of the 'kbd' package.

V-77071
Updated the check and fix to reference the correct location for the desired configuration settings.

V-77121
Corrected the "useauthtok" typo in the check and fix.

V-77137
Updated the command listed in the check.

V-77139
Updated the commands listed in the check and fix

V-77145
Updated the file paths in the check and fix

V-77183
Added a Not Applicable statement to the requirement.

V-77185
Added a Not Applicable statement to the requirement.

V-77237
Fixed typo in check text by replacing "nouid" with "nosuid"

V-77293
Updated the check and fix content to better address the requirement.

V-77297

Updated the check to verify the root account is assigned to an actual person. Updated the fix to include a command to implement changes to the /etc/aliases file.

V-77301
Updated the check and fix to ensure that the au-remote plugin was enabled.

V-77311
Updated the required permissions for /var/log/audit
Updated the Check and Fix to include "/etc/audit/rules.d/audit.rules"

V-77315
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77317
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77319
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77321
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77323
Updated the Check and Fix to be consistent with other Unix STIGs

V-77325
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77327
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77329
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77331
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77333
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77335

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules". Added "umount2" as a required audit rule.

V-77337

Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77339

Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77341

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77343

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77345

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77347

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77349

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77351

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77353

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77355

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77357

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77359

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77361

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77363

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77365

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77367

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77369

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77371

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77373

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77375

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77377

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77379

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77381

Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77383
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77385
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77387
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77389
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77391
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77393
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77395
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77397
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77399
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77401
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77403
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77405
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77407
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77409
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77411

Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77413
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77415
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77417
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77419
Removed the architecture references from the audit rule. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77421
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77423
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77425
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77427
Updated the finding statement to require both 32bit and 64bit rules are defined. Updated the fix to use "/etc/audit/rules.d/audit.rules"

V-77431
Updated the check and fix to use the correct configuration "banner_file".

V-77445
Updated the "Banner" file path in the check and fix

V-77469
Added a version check and a "Not Applicable" statement to the requirement

V-77475
Updated the example output and lowered the maximum allowable value for "maxpoll"

V-77479
Updated the commands in the Fix Text

V-77491
Updated the commands in the check and fix text.

V-77493
Updated the commands in the check and fix text.

V-77495
Updated the commands in the check and fix text.

V-77499
Updated the command in the check text.

V-77509
Updated the Vulnerability discussion. Corrected typo's in the check and fix text.

V-81709
Updated the check and fix to reference the correct location for the desired configuration settings.

V-81785
Updated the removal action in the fix text to reflect the correct file paths

V-97227
Added a new requirement to remove a default audit rule.

VMware vSphere 6.5 ESXi STIG, Version 1, Release 2

V-94049
Removed multiple duplicate requirements in ESXi STIG.

V-94485
Removed deprecated requirement V-94485.

V-94491
Removed multiple duplicate requirements in ESXi STIG.

V-94493
Removed multiple duplicate requirements in ESXi STIG.

V-94495
Removed multiple duplicate requirements in ESXi STIG.

V-94497
Removed multiple duplicate requirements in ESXi STIG.

V-94499
Removed multiple duplicate requirements in ESXi STIG.

V-94501
Removed multiple duplicate requirements in ESXi STIG.

V-94503
Removed multiple duplicate requirements in ESXi STIG.

V-94513
Removed multiple duplicate requirements in ESXi STIG.

V-94515
Removed multiple duplicate requirements in ESXi STIG.

V-94517
Removed multiple duplicate requirements in ESXi STIG.

V-94519
Removed multiple duplicate requirements in ESXi STIG.

V-94521
Removed multiple duplicate requirements in ESXi STIG.

V-94523
Removed multiple duplicate requirements in ESXi STIG.

V-94525
Removed multiple duplicate requirements in ESXi STIG.

V-94527
Removed multiple duplicate requirements in ESXi STIG.

V-94537
Removed multiple duplicate requirements in ESXi STIG.

V-94539
Removed multiple duplicate requirements in ESXi STIG.

V-94541
Removed multiple duplicate requirements in ESXi STIG.

V-94551
Removed multiple duplicate requirements in ESXi STIG.

V-94553
Removed multiple duplicate requirements in ESXi STIG.

V-94555
Removed multiple duplicate requirements in ESXi STIG.

V-94557
Removed multiple duplicate requirements in ESXi STIG.

VMware vSphere 6.5 Virtual Machine STIG, Version 1, Release 2

V-94573

Adjusted syntax in V-94573

V-94641

Removed multiple duplicate requirements in VMM STIG.

V-94643

Removed multiple duplicate requirements in VMM STIG.

V-94645

Removed multiple duplicate requirements in VMM STIG.

Voice Video Services Policy STIG, Version ersion 3 , Release elease 17

V-21507

V-21507 - requirement removed.

Windows 10 STIG, Version 1, Release 19

V-88203

V-88203 - Group Title: Rename from WN10-CC-000340 to WN10-CC-000360.

Windows Defender AV STIG Benchmark, Version 1, Release 4

Benchmark Update

Updated CPE OVAL to make the benchmark applicable to Windows Server 2016.

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

V-4448

Removed extraneous OVAL tests that were passing non-STIG-compliant settings.

Windows Server 2012 and 2012 R2 DC STIG, Version 2, Release 18

V-1135

V-1135 - Modify check text (Exclude Microsoft Print to PDF and Microsoft XPS Document Writer, which do not support sharing.)

Windows Server 2012 and 2012 R2 MS STIG Benchmark, Version 2, Release 17

V-4448

Removed extraneous OVAL tests that were passing non-STIG-compliant settings.

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

V-1135

V-1135 - Modify check text (Exclude Microsoft Print to PDF and Microsoft XPS Document Writer, which do not support sharing.)

z/OS BMC MAINVIEW for ACF2 STIG, Version 6, Release 9

V-16932

Mainview: Clarify use of Table 11-36 in Addendum

z/OS BMC MAINVIEW for RACF STIG, Version 6, Release 9

V-16932

Mainview: Clarify use of Table 11-36 in Addendum

z/OS BMC MAINVIEW for TSS STIG, Version 6, Release 9

V-16932

Mainview: Clarify use of Table 11-36 in Addendum

z/OS SRR Scripts, Version 6, Release 42

V-180

Corrected GENERIC (*) access being a finding in RACF.

V-18014

Changed requirement for CREATE option from UPDATE to CREATE.

Changed requirement for CREATE option from UPDATE to ALTER.

N/A

Errors in number of users within a group and Do Loop not being properly closed.