

October 2022 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Adobe Acrobat Reader DC Continuous Track STIG Benchmark, Version 2, Release 2

NA

Modified the OVAL-CPE to include detection for the 64-bit version.

Apple iOS 12 STIG, Version 2, Release 1

AIOS-12-999999

Added new requirement to sunset STIG.

Apple iOS/iPadOS 14 STIG, Version 1, Release 3

AIOS-14-999999

Added new requirement to sunset STIG.

Apple iOS/iPadOS 15 STIG, Version 1, Release 4

AIOS-15-012700

Corrected typo in verification procedure.

Apple macOS 12 (Monterey) STIG, Version 1, Release 4

APPL-12-000024

Updated check text to include sshd_config.d directories.

APPL-12-000051

Updated check text to include sshd_config.d directories.

APPL-12-000052

Updated check text to include sshd_config.d directories.

APPL-12-000053

Updated check text to include sshd_config.d directories.

APPL-12-001100

Updated check text to include sshd_config.d directories.

Application Security and Development STIG, Version 5, Release 2

APSC-DV-001795

Updated CCI reference.

APSC-DV-002880

Updated CCI reference.

APSC-DV-002890

Updated CCI reference.

APSC-DV-002900

Updated CCI reference.

APSC-DV-002910

Updated CCI reference.

APSC-DV-002920

Updated CCI reference.

APSC-DV-002930

Updated CCI reference.

APSC-DV-002950

Updated CCI reference.

APSC-DV-002960

Updated CCI reference.

APSC-DV-002970

Updated CCI reference.

APSC-DV-002980

Updated CCI reference.

APSC-DV-002990

Updated CCI reference.

APSC-DV-002995

Updated CCI reference.

APSC-DV-003000

Updated CCI reference.

APSC-DV-003010

Updated CCI reference.

APSC-DV-003020

Updated CCI reference.

APSC-DV-003040

Updated CCI reference.

APSC-DV-003050

Updated CCI reference.

APSC-DV-003060

Updated CCI reference.

APSC-DV-003070

Updated CCI reference.

APSC-DV-003080

Updated CCI reference.

APSC-DV-003090

Updated CCI reference.

APSC-DV-003100

Updated CCI reference.

APSC-DV-003120

Updated CCI reference.

APSC-DV-003130

Updated CCI reference.

APSC-DV-003140

Updated CCI reference.

APSC-DV-003150

Updated CCI reference.

APSC-DV-003160

Updated CCI reference.

APSC-DV-003170

Updated CCI reference.

APSC-DV-003180

Updated CCI reference.

APSC-DV-003190

Updated CCI reference.

APSC-DV-003200

Updated CCI reference.

APSC-DV-003210

Updated CCI reference.

APSC-DV-003215

Updated CCI reference.

APSC-DV-003220

Updated CCI reference.

APSC-DV-003230

Updated CCI reference.

APSC-DV-003235

Updated CCI reference.

APSC-DV-003236

Updated CCI reference.

APSC-DV-003240

Updated CCI reference.

APSC-DV-003250

Updated CCI reference.

APSC-DV-003260

Updated CCI reference.

APSC-DV-003270

Updated CCI reference.

APSC-DV-003280

Updated CCI reference.

APSC-DV-003285

Updated CCI reference.

APSC-DV-003290

Updated CCI reference.

APSC-DV-003300

Updated CCI reference.

APSC-DV-003310

Updated CCI reference.

APSC-DV-003320

Updated CCI reference.

APSC-DV-003330

Updated CCI reference.

APSC-DV-003340

Updated CCI reference.

APSC-DV-003345

Updated CCI reference.

APSC-DV-003350

Updated CCI reference.

APSC-DV-003400

Updated CCI reference.

APSC-DV-001860

Upgraded severity of control to a CAT I.

Application Server SRG, Version 3, Release 3**SRG-APP-000179-AS-000129**

Upgraded to CAT I per DISA RE.

SRG-APP-000224-AS-000152

Upgraded to CAT I per DISA RE.

SRG-APP-000391-AS-000239

Upgraded to CAT I per DISA RE.

SRG-APP-000392-AS-000240

Upgraded to CAT I per DISA RE.

SRG-APP-000149-AS-000102

Upgraded to CAT I per DISA RE.

SRG-APP-000151-AS-000103

Upgraded to CAT I per DISA RE.

CA IDMS STIG, Version 1, Release 2**IDMS-DB-000190**

Corrected the non-ASCII characters.

Canonical Ubuntu 18.04 LTS STIG, Version 2, Release 9**UBTU-18-010032**

Updated CCI.

UBTU-18-010021

Corrected typo in the check text and updated the fix text.

Canonical Ubuntu 20.04 LTS STIG, Version 1, Release 6**UBTU-20-010038**

Updated check text to include sshd_config.d directories.

UBTU-20-010044

Updated check text to include sshd_config.d directories.

UBTU-20-010033

Updated check text to include sshd_config.d directories.

UBTU-20-010035

Updated check text to include sshd_config.d directories.

UBTU-20-010036

Updated check text to include sshd_config.d directories.

UBTU-20-010037

Updated check text to include sshd_config.d directories.

UBTU-20-010043

Updated check text to include sshd_config.d directories.

UBTU-20-010047

Updated check text to include sshd_config.d directories.

UBTU-20-010048

Updated check text to include sshd_config.d directories.

UBTU-20-010049

Updated check text to include sshd_config.d directories.

UBTU-20-010453

Updated CCI.

UBTU-20-010415

Updated check and fix text.

Central Log Server SRG, Version 2, Release 2

SRG-APP-000125-AU-000310

Change SAMLI to SAMI in the Rule text.

Spelled out SAMI acronym.

Cisco ASA Firewall STIG, Version 1, Release 3

CASA-FW-000150

Added a note regarding multi-context mode.

CASA-FW-000220

Added a note regarding multi-context mode.

Added a note that 'shun' is optional.

CASA-FW-000300

Added a note regarding multi-context mode.

Cisco ASA NDM STIG, Version 1, Release 2

CASA-ND-001410

Mapped requirement to correct CCI.

Cisco IOS Router RTR STIG, Version 2, Release 2

CISC-RT-000270

Corrected typo in check and fix text.

CISC-RT-000070

Removed requirement; it is duplicated in NDM.

Cisco IOS Switch L2S STIG, Version 2, Release 3

CISC-L2-000020

Add CCI to requirement.

CISC-L2-000130

Added a note exempting 802.1x configured ports.

CISC-L2-000140

Added a note exempting 802.1x configured ports.

CISC-L2-000150

Added a note exempting 802.1x configured ports.

CISC-L2-000080

Removed requirement and rolled into CISC-L2-000020.

CISC-L2-000060

Removed capability requirement.

CISC-L2-000010

Removed requirement; it is duplicated in NDM.

Cisco IOS Switch RTR STIG, Version 2, Release 2

CISC-RT-000270

Corrected typo in check and fix text.

CISC-RT-000070

Removed requirement; it is duplicated in NDM.

Cisco IOS-XE Router NDM STIG, Version 2, Release 4

CISC-ND-001220

Added a note concerning control plane default policy.

Cisco IOS-XE Router RTR STIG, Version 2, Release 5

CISC-RT-000270

Corrected typo in check and fix text.

CISC-RT-000070

Removed requirement; it is duplicated in NDM.

Cisco IOS-XE Switch L2S STIG, Version 2, Release 3

CISC-L2-000020

Add CCI to requirement.

CISC-L2-000140

Added a note exempting 802.1x configured ports.

CISC-L2-000080

Removed requirement and rolled into CISC-L2-000020.

CISC-L2-000060

Removed capability requirement.

CISC-L2-000010

Removed requirement; it is duplicated in NDM.

CISC-L2-000090

Corrected rule title, check, and fix text.

Cisco IOS-XE Switch NDM STIG, Version 2, Release 4

CISC-ND-001220

Added a note concerning control plane default policy.

Cisco IOS-XE Switch RTR STIG, Version 2, Release 2

CISC-RT-000270

Corrected typo in check and fix text.

CISC-RT-000070

Removed requirement; it is duplicated in NDM.

Cisco ISE NAC STIG, Version 1, Release 4

CSCO-NC-000060

Remove the statement "This is required for compliance with C2C Step 1." and leave the statement "This is

Cisco ISE NDM STIG, Version 1, Release 4

CSCO-NM-000100

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000140

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000150

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000160

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000170

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000180

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000250

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000650

Update to remove WARN level. Both logging categories have INFO as the default log severity level and you.

CSCO-NM-000370 □

Change Check and Fix procedure to use state that configuring FIPS mode is the required DoD configuration,

CSCO-NM-000380 □

Changed FIPS mode language in check and fix.

CSCO-NM-000460 □

Changed FIPS mode language in check and fix.

CSCO-NM-000480 □

Changed FIPS mode language in check and fix.

CSCO-NM-000490 □

Changed FIPS mode language in check and fix.

CSCO-NM-000510 □

Changed FIPS mode language in check and fix.

CSCO-NM-000530 □

Changed FIPS mode language in check and fix.

Firewall SRG, Version 2, Release 3

SRG-NET-000333-FW-000014

Mapped requirement to correct CCI.

Fortinet FortiGate Firewall NDM STIG, Version 1, Release 3

FGFW-ND-000110

Updated check and fix text.

Fortinet FortiGate Firewall STIG, Version 1, Release 3

FNFG-FW-000045

Updated check and fix text.

Google Android 9 STIG, Version 2, Release 1**GOOG-09-999999**

Added new requirement to sunset STIG.

Google Chrome STIG, Version 2, Release 7**DTBC-0038**

Modified check and fix to reflect changes to the policy.

HBSS ePO 5.x STIG, Version 2, Release 9**H40180 - ePO 5x**

Updated check and fix text.

H34100 - ePO 5x

Updated finding statement for clarity.

HBSS McAfee Agent STIG, Version 5, Release 6**H35190**

Updated check and fix text.

H36120

Updated check and fix text.

IBM WebSphere Liberty Server STIG, Version 1, Release 2**IBMW-LS-000380**

Modified check and fix.

IBMW-LS-000390

Modified check and fix.

IBMW-LS-000450

Modified check and fix.

IBMW-LS-000770

Modified check and fix.

IBMW-LS-000790

Modified check and fix.

IBMW-LS-001120

Modified check and fix.

IBMW-LS-000381

Modified fix.

IBM-LS-000970

Modified fix.

IBM-LS-000010

Modified vul discussion.

IBM-LS-000260

Modified vul discussion.

IBM-LS-000020

Modified vul discussion, check, and fix.

IBM-LS-000030

Modified vul discussion, check, and fix.

IBM-LS-000040

Modified vul discussion, check, and fix.

IBM-LS-000320

Modified vul discussion, check, and fix.

IBM z/OS ACF2 STIG, Version 8, Release 8**ACF2-ES-000140**

Corrected the non-ASCII characters.

ACF2-TC-000010

Corrected the non-ASCII characters.

ACF2-TC-000030

Corrected the non-ASCII characters.

ACF2-ES-000860

Corrected the non-ASCII characters.

ACF2-ES-000760

Corrected the non-ASCII characters.

ACF2-FT-000040

Combined with ACF2-FT-000050.

ACF2-FT-000050

Removed requirement.

ACF2-TN-000040

ACF2-TN-000040 and ACF2-TN-000050

ACF2-TN-000050

Removed requirement.

ACF2-UT-000040

Combined with ACF2-UT-000050.

ACF2-UT-000050

Removed requirement.

ACF2-OS-000110

Edited rule title for clarity.

ACF2-ES-000960

Corrected Volmask typo.

ACF2-US-000160

Integrate this requirement into the ACF2 zOS STIG.

ACF2-ES-000770

Corrected the non-ASCII characters.

ACF2-FT-000090

Corrected the non-ASCII characters.

ACF2-SL-000030

Corrected the non-ASCII characters.

ACF2-TC-000070

Corrected the non-ASCII characters.

ACF2-US-000200

Corrected the non-ASCII characters.

ACF2-US-000230

Corrected the non-ASCII characters.

ACF2-CE-000030

Corrected the non-ASCII characters.

ACF2-ES-000090

Corrected the non-ASCII characters.

ACF2-ES-000180

Corrected the non-ASCII characters.

ACF2-ES-000210

Corrected the non-ASCII characters.

ACF2-ES-000270

Corrected the non-ASCII characters.

ACF2-ES-000340

Corrected the non-ASCII characters.

ACF2-ES-000880

Corrected the non-ASCII characters.

ACF2-FT-000010

Corrected the non-ASCII characters.

ACF2-FT-000100

Corrected the non-ASCII characters.

ACF2-IC-000030

Corrected the non-ASCII characters.

ACF2-JS-000050

Corrected the non-ASCII characters.

ACF2-JS-000060

Corrected the non-ASCII characters.

ACF2-OS-000160

Corrected the non-ASCII characters.

ACF2-OS-000250

Corrected the non-ASCII characters.

ACF2-SM-000020

Corrected the non-ASCII characters.

ACF2-SM-000050

Corrected the non-ASCII characters.

ACF2-TN-000060

Corrected the non-ASCII characters.

ACF2-TS-000010

Corrected the non-ASCII characters.

ACF2-US-000020

Corrected the non-ASCII characters.

ACF2-US-000030

Corrected the non-ASCII characters.

ACF2-US-000050

Corrected the non-ASCII characters.

ACF2-US-000070

Corrected the non-ASCII characters.

ACF2-US-000110

Corrected the non-ASCII characters.

ACF2-US-000140

Corrected the non-ASCII characters.

ACF2-US-000150

Corrected the non-ASCII characters.

ACF2-US-000170

Corrected the non-ASCII characters.

ACF2-US-000190

Corrected the non-ASCII characters.

IBM z/OS RACF STIG, Version 8, Release 8**RACF-IC-000030**

Corrected typo.

IBM z/OS TSS STIG, Version 8, Release 7**TSS0-UT-000040**

Removed banner statement from discussion.

TSS0-UT-000050

Removed banner statement from discussion.

IBM zVM Using CA VMSecure STIG, Version 2, Release 2**IBMZ-VM-000010**

Corrected the non-ASCII characters.

IBMZ-VM-000020

Corrected the non-ASCII characters.

IBMZ-VM-000030

Corrected the non-ASCII characters.

IBMZ-VM-000040

Corrected the non-ASCII characters.

IBMZ-VM-000050

Corrected the non-ASCII characters.

IBMZ-VM-000060

Corrected the non-ASCII characters.

IBMZ-VM-000070

Corrected the non-ASCII characters.

IBMZ-VM-000090

Corrected the non-ASCII characters.

IBMZ-VM-000110

Corrected the non-ASCII characters.

IBMZ-VM-000320

Corrected the non-ASCII characters.

IBMZ-VM-000460

Corrected the non-ASCII characters.

IBMZ-VM-000470

Corrected the non-ASCII characters.

IBMZ-VM-000480

Corrected the non-ASCII characters.

IBMZ-VM-000500

Corrected the non-ASCII characters.

IBMZ-VM-000510

Corrected the non-ASCII characters.

IBMZ-VM-000590

Corrected the non-ASCII characters.

IBMZ-VM-000600

Corrected the non-ASCII characters.

IBMZ-VM-000660

Corrected the non-ASCII characters.

IBMZ-VM-000680

Corrected the non-ASCII characters.

IBMZ-VM-000690

Corrected the non-ASCII characters.

IBMZ-VM-000710

Corrected the non-ASCII characters.

IBMZ-VM-000720

Corrected the non-ASCII characters.

IBMZ-VM-000730

Corrected the non-ASCII characters.

IBMZ-VM-000740

Corrected the non-ASCII characters.

IBMZ-VM-000750

Corrected the non-ASCII characters.

IBMZ-VM-000810

Corrected the non-ASCII characters.

IBMZ-VM-000830

Corrected the non-ASCII characters.

IBMZ-VM-000910

Corrected the non-ASCII characters.

IBMZ-VM-000930

Corrected the non-ASCII characters.

IBMZ-VM-000960

Corrected the non-ASCII characters.

IBMZ-VM-000980

Corrected the non-ASCII characters.

IBMZ-VM-000990

Corrected the non-ASCII characters.

IBMZ-VM-001020

Corrected the non-ASCII characters.

IBMZ-VM-001040

Corrected the non-ASCII characters.

IBMZ-VM-001060

Corrected the non-ASCII characters.

IBMZ-VM-001070

Corrected the non-ASCII characters.

IBMZ-VM-001090

Corrected the non-ASCII characters.

IBMZ-VM-001110

Corrected the non-ASCII characters.

IBMZ-VM-001120

Corrected the non-ASCII characters.

IBMZ-VM-001130

Corrected the non-ASCII characters.

IBMZ-VM-001140

Corrected the non-ASCII characters.

IBMZ-VM-001150

Corrected the non-ASCII characters.

IBMZ-VM-001210

Corrected the non-ASCII characters.

IBMZ-VM-001220

Corrected the non-ASCII characters.

IBMZ-VM-001230

Corrected the non-ASCII characters.

IBMZ-VM-001240

Corrected the non-ASCII characters.

IBMZ-VM-001250

Corrected the non-ASCII characters.

IBMZ-VM-001270

Corrected the non-ASCII characters.

Juniper Router NDM STIG, Version 2, Release 2**JUNI-ND-000490**

Corrected note in check and fix text.

Juniper SRX Services Gateway VPN STIG, Version 2, Release 2**JUSX-VN-000011**

Fixed mismatch between rule and check.

Kubernetes STIG, Version 1, Release 7**CNTR-K8-000320**

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000920

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000940

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001470

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001620

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002010

Add comments to check that PSP will be deprecated and to use the new Pod Security Admission Controller
Removed Master Node and replaced with "Control Plane".

CNTR-K8-002000

Add comments to check that PSP will be deprecated and to use the new Pod Security Admission Controller
Removed Master Node and replaced with "Control Plane".

CNTR-K8-002011

PSP has been deprecated; Kubernetes must have Pod Security Admission set.

CNTR-K8-002001

PSP has been deprecated; Kubernetes must have Pod Security Admission set.

CNTR-K8-000150

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000160

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000170

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000180

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000190

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000220

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000270

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000300

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000310

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000340

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000350

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000360

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000400

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000410

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000420

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000430

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000450

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000460

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000470

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000600

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000610

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000700

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000860

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000890

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000900

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000910

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000930

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000950

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000960

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001160

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001360

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001400

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001410

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001430

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001440

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001450

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001460

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001480

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001490

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001500

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001510

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001520

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001530

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001540

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001550

Removed Master Node and replaced with "Control Plane".

CNTR-K8-001990

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002600

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002700

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002720

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003110

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003120

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003130

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003140

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003150

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003160

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003170

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003250

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003260

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003270

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003280

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003290

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003300

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003310

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003320

Removed Master Node and replaced with "Control Plane".

CNTR-K8-003350

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002620

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002630

Removed Master Node and replaced with "Control Plane".

CNTR-K8-002640

Removed Master Node and replaced with "Control Plane".

CNTR-K8-000330

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-000370

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-000380

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-000440

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-000850

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-000880

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-001420

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

CNTR-K8-001300

Removed Master Node and replaced with "Control Plane". Changed check and fix to be accurate and

Mainframe Product SRG, Version 2, Release 1**SRG-APP-000004-MFP-000004**

Corrected the non-ASCII characters.

MarkLogic Server v9 STIG, Version 2, Release 1**ML09-00-012100**

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

ML09-00-012200

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

ML09-00-004800

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

ML09-00-004300

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

ML09-00-004000

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

ML09-00-012000

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

McAfee ENS 10.x Local Client STIG, Version 1, Release 3**NA**

Added statements regarding applicability of McAfee Agent STIG.

McAfee ENS 10.x STIG, Version 2, Release 9

NA

Added statements regarding applicability of McAfee Agent STIG.

TBD

Added requirement - the ENS Firewall rules must not allow all inbound traffic.

ENS-FW-000006

Removed allow-all rule from check text.

ENS-FW-000007

Removed allow-all rule from check text.

ENS-FW-000009

Updated discussion to better address FTP protocol inspection.

Microsoft .NET Framework 4 STIG Benchmark, Version 2, Release 2

APPNET0067

Modified OVAL logic to alleviate scanning errors when using McAfee Policy Auditor.

Microsoft .Net Framework 4.0 STIG, Version 2, Release 2

APPNET0066

Changed Check Text: If the "defaultProxy" element is empty or if "useSystemDefault =True", then the

Microsoft Edge STIG, Version 1, Release 6

EDGE-00-000064

Clarified check verbiage and downgraded severity to CAT III.

EDGE-00-000042

Clarified check verbiage and downgraded severity to CAT III.

EDGE-00-000039

Clarified check verbiage and downgraded severity to CAT III.

EDGE-00-000001

Corrected typos in vul discussion, check, and fix.

EDGE-00-000004

Clarified check verbiage and downgraded severity to CAT III.

Microsoft IIS 10.0 Server STIG, Version 2, Release 7

IIST-SV-000140

Altered check for the use of Custom Error Pages.

Microsoft IIS 10.0 Site STIG, Version 2, Release 7

IIST-SI-000230

Added a NA clause for WSUS.

IIST-SI-000233

Altered check for the use of Custom Error Pages.

IIST-SI-000257

Removed requirement.

Microsoft Internet Explorer 11 STIG Benchmark, Version 2, Release 3

DTBI1110-IE11

Modified OVAL logic removing unnecessary "OR" operator mitigating potential issues with some SCAP

Microsoft Internet Explorer 11 STIG, Version 2, Release 3

DTBI1115-IE11

Removed caveat verbiage.

DTBI1120-IE11

Removed caveat verbiage.

DTBI1125-IE11

Removed caveat verbiage.

DTBI1130-IE11

Removed caveat verbiage.

Microsoft Office 365 ProPlus STIG, Version 2, Release 7

O365-EX-000002

Updated check and fix text.

MongoDB Enterprise Advanced 4.x STIG, Version 1, Release 2

MD4X-00-000600

Changed severity to CAT1.

MD4X-00-001300

Changed severity to CAT1.

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MD4X-00-001600

Changed severity to CAT1.

MD4X-00-001700

Changed severity to CAT1.

MD4X-00-002100

Changed severity to CAT1.

MD4X-00-002950

Changed severity to CAT1.

MD4X-00-003000

Changed severity to CAT1.

MD4X-00-003100

Changed severity to CAT1.

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MD4X-00-003300

Changed severity to CAT1.

MD4X-00-003800

Changed severity to CAT1.

MD4X-00-006500

Changed severity to CAT1.

MD4X-00-003700

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

Motorola Android 9 COBO STIG, Version 1, Release 2

MOTO-09-999999

Added new requirement to sunset STIG.

Motorola Android 9 COPE STIG, Version 1, Release 2

MOTO-09-999999

Added new requirement to sunset STIG.

Mozilla Firefox STIG, Version 6, Release 4

FFOX-00-000016

Added "AO-Approved Certs" clause.

MS SQL Server 2014 Instance STIG, Version 2, Release 3

SQL4-00-031100

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MS SQL Server 2016 Database STIG, Version 2, Release 5

SQL6-D0-003200

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MS SQL Server 2016 Instance STIG, Version 2, Release 8

SQL6-D0-015700

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

SQL6-D0-008700

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

SQL6-D0-015800

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

SQL6-D0-008300

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

SQL6-D0-009200

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

SQL6-D0-008400

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

SQL6-D0-015600

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

Oracle Linux 7 STIG, Version 2, Release 9**OL07-00-010342**

Updated fix text.

OL07-00-010343

Updated check and fix text.

OL07-00-020023

Updated fix text.

OL07-00-010271

Added requirement to address emergency accounts.

OL07-00-040310

Corrected typo in the Vulnerability Discussion.

OL07-00-040360

Updated CCI.

OL07-00-040530

Updated CCI.

OL07-00-030201

Updated fix text.

OL07-00-021700

Updated check text command to eliminate false positives.

OL07-00-021040

Updated check text command to eliminate false positives.

OL07-00-040160

Updated check text.

OL07-00-030840

Updated check and fix text.

Oracle Linux 8 STIG, Version 1, Release 4

OL08-00-020140

Updated fix text.

OL08-00-020150

Updated fix text.

OL08-00-020160

Updated fix text.

OL08-00-020170

Updated fix text.

OL08-00-020230

Updated fix text.

OL08-00-020280

Updated fix text.

OL08-00-020300

Updated fix text.

OL08-00-020104

Updated check and fix text.

OL08-00-020110

Updated fix text.

OL08-00-020120

Updated fix text.

OL08-00-020130

Updated fix text.

OL08-00-010372

Updated fix text.

OL08-00-010373

Updated fix text.

OL08-00-010374

Updated fix text.

OL08-00-010375

Updated fix text.

OL08-00-010376

Updated fix text.

OL08-00-010383

Updated fix text.

OL08-00-010384

Updated fix text.

OL08-00-010430

Updated fix text.

OL08-00-010671

Updated fix text.

OL08-00-040209

Updated fix text.

OL08-00-040210

Updated fix text.

OL08-00-040220

Updated fix text.

OL08-00-040230

Updated fix text.

OL08-00-040239

Updated fix text.

OL08-00-040240

Updated fix text.

OL08-00-040249

Updated fix text.

OL08-00-040250

Updated fix text.

OL08-00-040259

Updated fix text.

OL08-00-040260

Updated fix text.

OL08-00-040261

Updated fix text.

OL08-00-040262

Updated fix text.

OL08-00-040270

Updated fix text.

OL08-00-040279

Updated fix text.

OL08-00-040280

Updated fix text.

OL08-00-040281

Updated fix text.

OL08-00-040282

Updated fix text.

OL08-00-040283

Updated fix text.

OL08-00-040284

Updated fix text.

OL08-00-040285

Updated fix text.

OL08-00-040286

Updated fix text.

OL08-00-010040

Updated check text to include sshd_config.d directories.

OL08-00-010200

Updated check text to include sshd_config.d directories and updated check and fix ClientAliveCountMax

OL08-00-010201

Updated check text to include sshd_config.d directories.

OL08-00-010500

Updated check text to include sshd_config.d directories.

OL08-00-010510

Updated check text to include sshd_config.d directories.

OL08-00-010520

Updated check text to include sshd_config.d directories.

OL08-00-010521

Updated check text to include sshd_config.d directories.

OL08-00-010522

Updated check text to include sshd_config.d directories.

OL08-00-010550

Updated check text to include sshd_config.d directories.

OL08-00-010830

Updated check text to include sshd_config.d directories.

OL08-00-020330

Updated check text to include sshd_config.d directories.

OL08-00-020350

Updated check text to include sshd_config.d directories and updated CCI.

OL08-00-040161

Updated check text to include sshd_config.d directories.

OL08-00-040340

Updated check text to include sshd_config.d directories.

OL08-00-040341

Updated check text to include sshd_config.d directories.

OL08-00-020340

Updated CCI.

OL08-00-020190

Fixed typo in the Rule Title.

OL08-00-040137

Updated check and fix text.

OL08-00-020352

Updated check text command to eliminate false positives.

OL08-00-020090

Updated check text and added NA statement.

OL08-00-010400

Updated check text and added NA statement.

OL08-00-010090

Updated check text and added NA statement.

Oracle MySQL 8.0 STIG, Version 1, Release 3

MYS8-00-007000

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MYS8-00-011800

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MYS8-00-004800

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MYS8-00-011600

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MYS8-00-006200

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MYS8-00-011500

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

MYS8-00-011700

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

Palo Alto ALG STIG, Version 2, Release 3

PANW-AG-000148

Updated to reflect this is not a finding if the protocol is not used in the implementation.

Palo Alto IDPS STIG, Version 2, Release 3

PANW-IP-000033

Updated check and fix method for creating the vulnerability profile.

Palo Alto NDM STIG, Version 2, Release 2

PANW-NM-000075 □

Corrected the check and fix to address the requirement that the neither the SA nor the Cryptographic

Red Hat Enterprise Linux 7 STIG, Version 3, Release 9

RHEL-07-010342

Updated fix text.

RHEL-07-010343

Updated fix text.

RHEL-07-020023

Updated fix text.

RHEL-07-040530

Updated CCI.

RHEL-07-010271

Added requirement to address emergency accounts.

RHEL-07-040310

Corrected typo in the Vulnerability Discussion.

RHEL-07-040360

Updated CCI.

RHEL-07-030201

Updated fix text.

RHEL-07-021700

Updated check text command to eliminate false positives.

RHEL-07-021040

Updated check text command to eliminate false positives.

RHEL-07-040160

Updated check text.

RHEL-07-030840

Updated check and fix text.

Red Hat Enterprise Linux 8 STIG, Version 1, Release 8

RHEL-08-010400

Updated check text and added NA statement.

RHEL-08-020104

Updated check and fix text.

RHEL-08-010090

Updated check text and added NA statement.

RHEL-08-020140

Updated fix text.

RHEL-08-040137

Updated check and fix text.

RHEL-08-020221

Fixed typo in check text.

RHEL-08-010383

Updated fix text.

RHEL-08-010384

Updated fix text.

RHEL-08-010671

Updated fix text.

RHEL-08-020300

Updated fix text.

RHEL-08-020130

Updated fix text.

RHEL-08-020150

Updated fix text.

RHEL-08-020160

Updated fix text.

RHEL-08-020170

Updated fix text.

RHEL-08-020230

Updated fix text.

RHEL-08-020280

Updated fix text.

RHEL-08-020110

Updated fix text.

RHEL-08-020120

Updated fix text.

RHEL-08-010372

Updated fix text.

RHEL-08-010373

Updated fix text.

RHEL-08-010374

Updated fix text.

RHEL-08-010375

Updated fix text.

RHEL-08-010376

Updated fix text.

RHEL-08-010430

Updated fix text.

RHEL-08-040209

Updated fix text.

RHEL-08-040210

Updated fix text.

RHEL-08-040220

Updated fix text.

RHEL-08-040230

Updated fix text.

RHEL-08-040239

Updated fix text.

RHEL-08-040240

Updated fix text.

RHEL-08-040249

Updated fix text.

RHEL-08-040250

Updated fix text.

RHEL-08-040259

Updated fix text.

RHEL-08-040260

Updated fix text.

RHEL-08-040261

Updated fix text.

RHEL-08-040262

Updated fix text.

RHEL-08-040270

Updated fix text.

RHEL-08-040279

Updated fix text.

RHEL-08-040280

Updated fix text.

RHEL-08-040281

Updated fix text.

RHEL-08-040282

Updated fix text.

RHEL-08-040283

Updated fix text.

RHEL-08-040284

Updated fix text.

RHEL-08-040285

Updated fix text.

RHEL-08-040286

Updated fix text.

RHEL-08-010040

Updated check text to include sshd_config.d directories.

RHEL-08-010200

Updated check text to include sshd_config.d directories and updated check and fix ClientAliveCountMax

RHEL-08-010500

Updated check text to include sshd_config.d directories and updated ClientAliveCountMax value to 1.

RHEL-08-010510

Updated check text to include sshd_config.d directories.

RHEL-08-010520

Updated check text to include sshd_config.d directories.

RHEL-08-010521

Updated check text to include sshd_config.d directories.

RHEL-08-010550

Updated check text to include sshd_config.d directories.

RHEL-08-010830

Updated check text to include sshd_config.d directories.

RHEL-08-020330

Updated check text to include sshd_config.d directories.

RHEL-08-020350

Updated check text to include sshd_config.d directories and updated CCI.

RHEL-08-040161

Updated check text to include sshd_config.d directories.

RHEL-08-040340

Updated check text to include sshd_config.d directories.

RHEL-08-040341

Updated check text to include sshd_config.d directories.

RHEL-08-010201

Updated check text to include sshd_config.d directories.

RHEL-08-010522

Updated check text to include sshd_config.d directories.

RHEL-08-010360

Fixed check text typo.

RHEL-08-020340

Updated CCI.

RHEL-08-020190

Fixed typo in the Rule Title.

RHEL-08-020352

Updated check text command to eliminate false positives.

RHEL-08-010000

Updated check text and Vulnerability Discussion.

RHEL-08-020090

Updated check text and added NA statement.

RHEL-08-040400

Added requirement for SELinux user mapping.

RD6X-00-009800

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-011600

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-010400

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-009200

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-009500

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-009900

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-010500

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-010000

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

RD6X-00-011700

Cryptographic modules should require either FIPS 140-2 or FIPS 140-3 validation.

Solaris 10 SPARC STIG Benchmark, Version 2, Release 3**GEN004360**

Modified OVAL logic to check both the aliases file and alises.db and to include new applicability checks.

GEN004370

Created OVAL content to verify both the aliases file and alises.db used by sendmail are group owned by root,

GEN004380

Created OVAL content to verify file permissions of the aliases file and aliases.db used by sendmail.

GEN004390

Created OVAL content to verify if there is an extended ACL for the aliases file and aliases.db used by

Solaris 10 SPARC STIG, Version 2, Release 3**GEN004360**

Updated check text and added NA statement.

GEN004370

Updated check text and added NA statement.

GEN004380

Updated check text and added NA statement.

GEN004390

Updated check text and added NA statement.

Solaris 10 X86 STIG Benchmark, Version 2, Release 3**GEN004360**

Modified OVAL logic to check both the aliases file and alises.db and to include new applicability checks.

GEN004370

Created OVAL content to verify both the aliases file and alises.db used by sendmail are group owned by root,

GEN004380

Created OVAL content to verify file permissions of the aliases file and aliases.db used by sendmail.

GEN004390

Created OVAL content to verify if there is an extended ACL for the aliases file and aliases.db used by

Solaris 10 x86 STIG, Version 2, Release 3**GEN004360**

Updated check text and added NA statement.

GEN004370

Updated check text and added NA statement.

GEN004380

Updated check text and added NA statement.

GEN004390

Updated check text and added NA statement.

SUSE Linux Enterprise Server 12 STIG, Version 2, Release 8**SLES-12-010390**

Updated CCI.

SLES-12-030130

Updated CCI.

SUSE Linux Enterprise Server 15 STIG, Version 1, Release 8**SLES-15-020080**

Updated CCI.

SLES-15-020120

Updated CCI.

TBD, TBD

TBD

Added automation to requirements previously not automated.

Traditional Security Checklist, Version 2, Release 3

NA

Added Traditional Security Overview.

IS-03.02.01

Added updated reference with requirements.

IA-10.02.02

Removed outdated information.

CS-04.01.04

Updated the check to include new requirements for PDS manhole covers.

VMware vSphere 6.7 Photon OS STIG, Version 1, Release 5

PHTN-67-000021

Added a note to check to state reboot is required.

PHTN-67-000031

Added a note to check to state reboot is required.

PHTN-67-000052

Added a note to check to state reboot is required.

PHTN-67-000075

Added a note to check to state reboot is required.

PHTN-67-000117

Added a note to check to state reboot is required.

PHTN-67-000082

Removed requirement.

VMware vSphere 6.7 vCenter STIG, Version 1, Release 3

VCTR-67-000009

Modified check and fix.

Web Server SRG, Version 3, Release 1

SRG-APP-000224-WSR-000135

Upgraded to CAT I per DISA RE.

SRG-APP-000179-WSR-000110

Upgraded to CAT I per DISA RE.

z/OS SRR Scripts, Version 6, Release 55

NA

Corrective action taken.

ACF2-ES-000820

Corrected issue with special characters in password.

ACF2-ES-000770

New automation.

ACF2-FT-000090

New automation.

ZWMQ0060

Corrective action taken.

RACF-FT-000100

New automation.

TSS0-FT-000070

New automation.

RACF-US-000240

New automation.

TSS0-US-000220

New automation.

Zebra Android 10 COBO STIG, Version 1, Release 2**ZEBR-10-999999**

Added new requirement to sunset STIG.

Zebra Android 10 COPE STIG, Version 1, Release 2**ZEBR-10-999999**

Added new requirement to sunset STIG.