

January 2022 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Apache Server 2.4 UNIX Server STIG, Version 2, Release 4

AS24-U1-000030

Corrected check text to meet intent.

Apache Tomcat Application Sever 9 STIG, Version 2, Release 4

TCAT-AS-001470

Modified check text to account for corrections required by TCAT-AS-000950.

Apple iOS/iPadOS 15 STIG, Version 1, Release 2

AIOS-15-012700

Fixed typos in Check text.

AIOS-15-013000

Fixed typos in Check text.

Apple macOS 10.13 STIG, Version 2, Release 4

AOSX-13-000475

Removed deprecated command from the STIG.

AOSX-13-000490

Removed deprecated command from the STIG.

Apple macOS 10.14 STIG, Version 2, Release 5

AOSX-14-002010

Removed deprecated command from the STIG.

AOSX-14-002011

Removed deprecated command from the STIG.

AOSX-14-002019

Removed deprecated command from the STIG.

Apple macOS 10.15 STIG, Version 1, Release 7

AOSX-15-002010

Removed deprecated command from the STIG.

AOSX-15-002011

Removed deprecated command from the STIG.

AOSX-15-002019

Removed deprecated command from the STIG.

AOSX-15-002070

Updated the requirement to allow for the use of the built-in MRT application or a third-party product.

Apple macOS 11 (Big Sur) STIG, Version 1, Release 5**APPL-11-002010**

Removed deprecated command from the STIG.

APPL-11-002011

Removed deprecated command from the STIG.

APPL-11-002019

Removed deprecated command from the STIG.

APPL-11-002070

Updated the requirement to allow for the use of the built-in MRT application or a third-party product.

Apple macOS 11 (Big Sur), Version 1, Release 4**APPL-11-000051**

Updated the vulnerability discussion and added a Not Applicable statement to the check.

APPL-11-000052

Updated the vulnerability discussion and added a Not Applicable statement to the check.

APPL-11-000053

Updated the vulnerability discussion and added a Not Applicable statement to the check.

Application Server SRG, Version 3, Release 2**SRG-APP-000133-AS-000093**

Remapped CCI for SRG-APP-000133-AS-000093.

Canonical Ubuntu 18.04 LTS STIG, Version 2, Release 5**UBTU-18-010501**

Updated the allowable values for "maxpoll" to be congruent with other Linux guidance.

UBTU-18-010001

Updated the directory path for the configuration file in the check text. Updated the grub update command in

UBTU-18-010522

Added a requirement to check for passwordless accounts.

UBTU-18-010523

Added a requirement to check for "nullok" in the /etc/pam.d/common_password file.

UBTU-18-010321

Combined similar syscall rules with this requirement.

UBTU-18-010322

Combined requirement with similar syscall rule.

UBTU-18-010325

Combined requirement with similar syscall rule.

UBTU-18-010326

Combined requirement with similar syscall rule.

UBTU-18-010327

Combined similar syscall rules with this requirement.

UBTU-18-010328

Combined requirement with similar syscall rule.

UBTU-18-010329

Combined requirement with similar syscall rule.

UBTU-18-010330

Combined requirement with similar syscall rule.

UBTU-18-010331

Combined similar syscall rules with this requirement.

UBTU-18-010332

Combined requirement with similar syscall rule.

UBTU-18-010333

Combined requirement with similar syscall rule.

UBTU-18-010334

Combined similar syscall rules with this requirement.

UBTU-18-010338

Combined requirement with similar syscall rule.

UBTU-18-010339

Combined requirement with similar syscall rule.

UBTU-18-010368

Combined requirement with similar syscall rule.

UBTU-18-010369

Combined requirement with similar syscall rule.

UBTU-18-010375

Combined similar syscall rules with this requirement.

UBTU-18-010376

Combined requirement with similar syscall rule.

UBTU-18-010377

Combined requirement with similar syscall rule.

UBTU-18-010378

Combined requirement with similar syscall rule.

UBTU-18-010323

Combined requirement with similar syscall rule.

UBTU-18-010324

Combined requirement with similar syscall rule.

UBTU-18-010370

Combined requirement with similar syscall rule.

UBTU-18-010382

Combined requirement with similar syscall rule.

UBTU-18-010383

Combined requirement with similar syscall rule.

UBTU-18-010384

Combined requirement with similar syscall rule.

Canonical Ubuntu 18.04 STIG Benchmark, Version 2, Release 5**UBTU-18-010321**

Modified OVAL logic in accordance with manual STIG update.

UBTU-18-010322

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010325

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010326

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010327

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010328

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010329

Modified OVAL logic logic in accordance with manual STIG update.

UBTU-18-010330

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010331

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010332

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010333

Modified OVAL logic logic in accordance with manual STIG update.

UBTU-18-010334

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010338

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010339

Modified OVAL logic logic in accordance with manual STIG update.

UBTU-18-010368

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010369

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010375

Modified OVAL logic logic in accordance with manual STIG update.

UBTU-18-010376

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010377

Removed OVAL content for rule in accordance with rule removal from manual STIG.

UBTU-18-010378

Removed OVAL content for rule in accordance with rule removal from manual STIG.

Canonical Ubuntu 20.04 LTS STIG, Version 1, Release 2

UBTU-20-010142

Combined similar syscall rules with this requirement.

UBTU-20-010143

Combined requirement with similar syscall rule.

UBTU-20-010144

Combined requirement with similar syscall rule.

UBTU-20-010145

Combined requirement with similar syscall rule.

UBTU-20-010146

Combined requirement with similar syscall rule.

UBTU-20-010147

Combined requirement with similar syscall rule.

UBTU-20-010148

Combined similar syscall rules with this requirement.

UBTU-20-010149

Combined requirement with similar syscall rule.

UBTU-20-010150

Combined requirement with similar syscall rule.

UBTU-20-010151

Combined requirement with similar syscall rule.

UBTU-20-010152

Combined similar syscall rules with this requirement.

UBTU-20-010153

Combined requirement with similar syscall rule.

UBTU-20-010154

Combined requirement with similar syscall rule.

UBTU-20-010155

Combined similar syscall rules with this requirement.

UBTU-20-010156

Combined requirement with similar syscall rule.

UBTU-20-010157

Combined requirement with similar syscall rule.

UBTU-20-010158

Combined requirement with similar syscall rule.

UBTU-20-010159

Combined requirement with similar syscall rule.

UBTU-20-010160

Combined requirement with similar syscall rule.

UBTU-20-010179

Combined similar syscall rules with this requirement.

UBTU-20-010180

Combined requirement with similar syscall rule.

UBTU-20-010267

Combined similar syscall rules with this requirement.

UBTU-20-010268

Combined requirement with similar syscall rule.

UBTU-20-010269

Combined requirement with similar syscall rule.

UBTU-20-010270

Combined requirement with similar syscall rule.

UBTU-20-010461

Added a requirement to prevent the automounting of USB storage devices.

UBTU-20-010462

Added a requirement to check for passwordless accounts.

UBTU-20-010463

Added a requirement to check for "nullok" in the /etc/pam.d/common_password file.

UBTU-20-010435

Updated the allowable values for "maxpoll" to be congruent with other Linux guidance.

Cisco IOS Router NDM STIG, Version 2, Release 3

CISC-ND-001200

Updated requirement to replace SHA-1 references with SHA-2.

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

CISC-ND-001030

Updated the regular expression used by the OVAL to check for ntp server addresses to accept additional

Cisco ISE NAC STIG, Version 1, Release 3

CSCO-NC-000030

Add C2C step to the requirement and check fields.

CSCO-NC-000040

Add C2C step to the requirement and check fields.

CSCO-NC-000050

Add C2C step to the requirement and check fields.

CSCO-NC-000060

Add C2C step to the requirement and check fields.

CSCO-NC-000070

Add C2C step to the requirement and check fields.

CSCO-NC-000080

Add C2C step to the requirement and check fields.

CSCO-NC-000090

Add C2C step to the requirement and check fields.

CSCO-NC-000100

Add C2C step to the requirement and check fields.

CSCO-NC-000110

Add C2C step to the requirement and check fields.

CSCO-NC-000120

Add C2C step to the requirement and check fields.

CSCO-NC-000130

Add C2C step to the requirement and check fields.

CSCO-NC-000250

Add C2C step to the requirement and check fields.

CSCO-NC-000310

Add C2C step to the requirement and check fields.

CSCO-NC-000320

Add C2C step to the requirement and check fields.

CSCO-NC-000260

Add C2C step to the requirement and check fields.

CSCO-NC-000180

Add C2C step to the requirement and check fields.

CSCO-NC-000190

Add C2C step to the requirement and check fields.

CSCO-NC-000200

Add C2C step to the requirement and check fields.

CSCO-NC-000210

Add C2C step to the requirement and check fields.

CSCO-NC-000220

Add C2C step to the requirement and check fields.

CSCO-NC-000270

Add C2C step to the requirement and check fields.

CSCO-NC-000280

Add C2C step to the requirement and check fields.

CSCO-NC-000290

Add C2C step to the requirement and check fields.

CSCO-NC-000300

Add C2C step to the requirement and check fields.

CSCO-NC-000140

Add C2C step to the requirement and check fields.

CSCO-NC-000010

Add C2C step to the requirement and check fields.

CSCO-NC-000020

Add C2C step to the requirement and check fields.

CSCO-NC-000150

Add C2C step to the requirement and check fields.

CSCO-NC-000160

Add C2C step to the requirement and check fields.

CSCO-NC-000170

Add C2C step to the requirement and check fields.

CSCO-NC-000230

Add C2C step to the requirement and check fields.

CSCO-NC-000240

Add C2C step to the requirement and check fields.

CVAD-DC-000030

Altered fix.

Citrix Virtual Apps and Desktop 7.x Workspace App STIG, Version 1, Release 2**CVAD-WS-000030**

Removed requirement.

Container Platform SRG, Version 1, Release 3**SRG-APP-000190-CTR-000500**

Added requirement to STIG.

SRG-APP-000439-CTR-001080

Added requirement to STIG.

Database SRG, Version 3, Release 2**SRG-APP-000456-DB-000400**

Changed requirement to a severity of CAT I and updated Check text.

SRG-APP-000023-DB-000001

Changed requirement to a severity of CAT I.

SRG-APP-000033-DB-000084

Changed requirement to a severity of CAT I.

SRG-APP-000133-DB-000198

Changed requirement to a severity of CAT I.

SRG-APP-000164-DB-000401

Changed requirement to a severity of CAT I.

SRG-APP-000171-DB-000074

Changed requirement to a severity of CAT I.

SRG-APP-000172-DB-000075

Changed requirement to a severity of CAT I.

SRG-APP-000176-DB-000068

Changed requirement to a severity of CAT I.

SRG-APP-000178-DB-000083

Changed requirement to a severity of CAT I.

SRG-APP-000179-DB-000114

Changed requirement to a severity of CAT I.

SRG-APP-000231-DB-000154

Changed requirement to a severity of CAT I.

SRG-APP-000416-DB-000380

Changed requirement to a severity of CAT I.

Forescout NAC STIG, Version 1, Release 3

FORE-NC-000270

Add C2C step to the requirement and check fields.

FORE-NC-000280

Add C2C step to the requirement and check fields.

FORE-NC-000230

Add C2C step to the requirement and check fields.

FORE-NC-000340

Add C2C step to the requirement and check fields.

FORE-NC-000470

Add C2C step to the requirement and check fields.

FORE-NC-000010

Add C2C step to the requirement and check fields.

FORE-NC-000020

Add C2C step to the requirement and check fields.

FORE-NC-000030

Add C2C step to the requirement and check fields.

FORE-NC-000040

Add C2C step to the requirement and check fields.

FORE-NC-000050

Add C2C step to the requirement and check fields.

FORE-NC-000060

Add C2C step to the requirement and check fields.

FORE-NC-000070

Add C2C step to the requirement and check fields.

FORE-NC-000080

Add C2C step to the requirement and check fields.

FORE-NC-000090

Add C2C step to the requirement and check fields.

FORE-NC-000100

Add C2C step to the requirement and check fields.

FORE-NC-000110

Add C2C step to the requirement and check fields.

FORE-NC-000440

Add C2C step to the requirement and check fields.

FORE-NC-000450

Add C2C step to the requirement and check fields.

FORE-NC-000210

Add C2C step to the requirement and check fields.

FORE-NC-000150

Add C2C step to the requirement and check fields.

FORE-NC-000160

Add C2C step to the requirement and check fields.

FORE-NC-000170

Add C2C step to the requirement and check fields.

FORE-NC-000420

Add C2C step to the requirement and check fields.

FORE-NC-000180

Add C2C step to the requirement and check fields.

FORE-NC-000190

Add C2C step to the requirement and check fields.

FORE-NC-000240

Add C2C step to the requirement and check fields.

FORE-NC-000460

Add C2C step to the requirement and check fields.

FORE-NC-000120

Add C2C step to the requirement and check fields.

FORE-NC-000130

Add C2C step to the requirement and check fields.

FORE-NC-000140

Add C2C step to the requirement and check fields.

FORE-NC-000290

Add C2C step to the requirement and check fields.

FORE-NC-000260

Add C2C step to the requirement and check fields.

Google Chrome Current Windows STIG Benchmark, Version 2, Release 5**DTBC-0056**

Added OVAL automation for rule.

Google Chrome STIG, Version 2, Release 5**DTBC-0065**

Corrected policy name.

DTBC-0074

Corrected syntax.

HBSS ePO 5.x STIG, Version 2, Release 6**H40300 - ePO 5x**

Corrected V-14507 reference to V-213249.

H30120 - ePO 5x

Updated client-side targeting.

H30700 - ePO 5x

Updated requirement for clarity.

H36220 - ePO 5x

Updated instructions in check text.

H90300 - ePO 5x

Updated to include conditions for cloud-hosted platforms.

HBSS HIP 8 Firewall STIG, Version 2, Release 1**H37060 - HIP 8 FW**

Added requirement for EOL Product.

HBSS HIP 8 STIG, Version 5, Release 2**H30280 - HIP 8**

Updated severity to CAT I; product is EOL.

HBSS McAfee Agent STIG, Version 5, Release 5**H36140**

Corrected instructions for navigating the menu.

HPE 3PAR StoreServ 3.2.x STIG, Version 2, Release 1

HP3P-32-001005

Removed requirement.

IBM AIX 7.x STIG, Version 2, Release 4**AIX7-00-003062**

Added a Not Applicable statement to the requirement for systems utilizing IPv6.

AIX7-00-001032

Updated check comands to search `"/root"` instead of `"/home/root"`.

AIX7-00-001130

Updated the example text in the check to reflect the correct value for `"default minspecialchar"` to 1.

IBM CICS Transaction Server for RACF STIG, Version 6, Release 7**ZCIC0041**

Modified the Release Number.

IBM CICS Transaction Server for TSS STIG, Version 6, Release 7**ZCIC0041**

Modified the Release Number.

IBM z/OS ACF2 STIG, Version 8, Release 5**ACF2-OS-000330**

Changed title to allow Key Storage in IBM ICSF; updated check and fix.

ACF2-ES-000140

Modified check and fix to address SMS managed catalogs.

ACF2-ES-000230

Modified Check and Fix to allow Site authorization in the SSP for consoles.

ACF2-TC-000010

Modified check and fix to include AT-TLS.

ACF2-TC-000080

Removed requirement. This is a duplicate of ACF2-TC-000010.

ACF2-TC-000030

Modified check and fix to include EZB.INITSTACK to SERVAUTH.

ACF2-TC-000100

Added requirement for Policy Agent configuration.

IBM z/OS RACF STIG, Version 8, Release 6**RACF-SH-000060**

Changed title to allow Key Storage in IBM ICSF; updated check and fix.

RACF-ES-000210

Modified check and fix to address SMS managed catalogs.

RACF-ES-000410

Modified Check and Fix to allow Site authorization in the SSP for consoles.

RACF-TC-000010

Modified check and fix to include AT-TLS.

RACF-TC-000050

Modified check and fix to include EZB.INITSTACK to SERVAUTH.

RACF-TC-000110

Added requirement for Policy Agent configuration.

IBM z/OS TSS STIG, Version 8, Release 5**TSS0-ES-000100**

Changed title to allow Key Storage in IBM ICSF; updated check and fix.

TSS0-ES-000320

Modified check and fix to address SMS managed catalogs.

TSS0-ES-000460

Modified Check and Fix to allow Site authorization in the SSP for consoles.

TSS0-ES-000860

Corrected contradicting typo in Rule Title.

TSS0-TC-000010

Modified check and fix to include AT-TLS.

TSS0-TC-000090

Removed requirement. This is a duplicate of TSS0-TC-000010.

TSS0-TC-000030

Modified check and fix to include EZB.INITSTACK to SERVAUTH.

TSS0-TC-000100

Added requirement for Policy Agent configuration.

IBM z/OS WebsphereMQ for ACF2 STIG, Version 6, Release 3**ZWMQ0011**

Modified Check and Fix to require encryption inside enclave.

IBM z/OS WebsphereMQ for RACF STIG, Version 6, Release 3**ZWMQ0011**

Modified Check and Fix to require encryption inside enclave.

IBM z/OS WebsphereMQ for TSS STIG, Version 6, Release 3

ZWMQ0011

Modified Check and Fix to require encryption inside enclave.

JBoss EAP 6.3 STIG, Version 2, Release 3

JBOS-AS-000015

Clarified discussion verbiage.

Kubernetes STIG, Version 1, Release 4

CNTR-K8-001520

Changed control to look for setting in kube-apiserver.yaml.

CNTR-K8-001530

Changed control to look for setting in kube-apiserver.yaml.

CNTR-K8-001510

Changed control to look for setting in kube-apiserver.yaml.

CNTR-K8-001450

Changed control to look for this setting in etcd.yaml. Changed discussion to reflect correct parameter.

CNTR-K8-001500

Changed control to refer to cert-file, not certfile, and to look for setting in Kubernetes etcd manifest.

CNTR-K8-001490

Changed control to refer to key-file, not keyfile, and to look for setting in Kubernetes etcd manifest.

CNTR-K8-001550

Changed discussion to reflect correct parameter.

CNTR-K8-001540

Changed discussion to reflect correct parameter.

CNTR-K8-002010

Removed deprecated Docker entry.

CNTR-K8-000320

Removed deprecated --insecure-port.

CNTR-K8-000920

Removed deprecated --insecure-port.

CNTR-K8-000940

Removed deprecated --insecure-port.

McAfee ENS 10.x STIG, Version 2, Release 6

ENS-EP-000001

Removed HIPS and Enable Adaptive Mode criteria.

ENS-TP-000243

Removed HIPS criteria.

ENS-TP-000241

Removed HIPS criteria.

ENS-TP-000239

Removed HIPS criteria.

ENS-TP-000238

Removed HIPS criteria.

ENS-CO-000100

Removed HIPS criteria.

ENS-TP-000246

Updated DAT file criterion to include ENSL.

McAfee MOVE Agentless 3.0 VSEL 1.9 for SVA STIG, Version 2, Release 1**DTAVSEL-114**

Added requirement for EOL Product.

McAfee MOVE Agentless 3.6.1 Security Virtual Appliance STIG, Version 2, Release 1**AV-MOVE-SVA-120**

Added requirement for EOL Product.

McAfee MOVE AV Agentless 4.5 STIG, Version 2, Release 1**MV45-GEN-200003**

Added requirement for EOL Product.

McAfee MOVE AV Multi-Platform 4.5 STIG, Version 2, Release 1**MV45-GEN-200003**

Added requirement for EOL Product.

McAfee VirusScan 8.8 Local Client STIG, Version 6, Release 1**DTAM171**

Added requirement for EOL Product.

McAfee VirusScan 8.8 Managed Client STIG, Version 6, Release 1**DTAM171**

Added requirement for EOL Product.

McAfee VSEL 1.9/2.0 Local Client STIG, Version 2, Release 1**DTAVSEL-302**

Added requirement for EOL Product.

McAfee VSEL 1.9/2.0 Managed Client STIG, Version 2, Release 1

DTAVSEL-302

Added requirement for EOL Product.

Microsoft Edge STIG, Version 1, Release 4

EDGE-00-000064

Added requirement Autoplay Allowlist.

Microsoft IIS 10.0 Server STIG, Version 2, Release 5

IIST-SV-000205

Reinstated N/A clause.

Microsoft IIS 10.0 Site STIG, Version 2, Release 5

IIST-SI-000255

Altered check and fix.

IIST-SI-000221

Altered finding statement.

IIST-SI-000236

Altered discussion.

Microsoft IIS 8.5 Site STIG, Version 2, Release 5

IISW-SI-000251

Altered check.

IISW-SI-000255

Altered check and fix.

Microsoft Office 365 ProPlus STIG, Version 2, Release 4

O365-CO-000013

Corrected "Load Controls in Forms3" check text criteria.

O365-AC-000003

Corrected inconsistencies across registry values.

O365-EX-000002

Corrected inconsistencies across registry values.

O365-PR-000003

Corrected inconsistencies across registry values.

O365-PT-000001

Corrected inconsistencies across registry values.

O365-PU-000003

Corrected inconsistencies across registry values.

O365-VI-000001

Corrected inconsistencies across registry values.

O365-WD-000018

Corrected inconsistencies across registry values.

O365-CO-000005

Corrected inconsistencies across registry values.

O365-CO-000027

Corrected inconsistencies across registry values.

O365-EX-000030

Corrected inconsistencies across registry values.

O365-OU-000001

Corrected inconsistencies across registry values.

O365-OU-000009

Corrected inconsistencies across registry values.

O365-OU-000010

Corrected inconsistencies across registry values.

O365-OU-000013

Corrected inconsistencies across registry values.

O365-OU-000014

Corrected inconsistencies across registry values.

O365-OU-000018

Corrected inconsistencies across registry values.

O365-PU-000001

Corrected inconsistencies across registry values.

O365-CO-000007

Corrected expected registry value for 'automationsecuritypublisher'.

Microsoft Office System 2016 STIG, Version 2, Release 2**DT00192**

Corrected "Load Controls in Forms3" check text criteria.

Microsoft SQL Server 2014 Instance STIG, Version 2, Release 2

SQL4-00-017410

Removed Windows from rule title.

SQL4-00-013600

Updated logic in check based on Windows behavior.

Microsoft SQL Server 2016 Database STIG, Version 2, Release 3**SQL6-D0-001100**

Corrected script in check.

Microsoft SQL Server 2016 Instance STIG, Version 2, Release 6**SQL6-D0-003800**

Corrected setspn commands in the fix.

SQL6-D0-003600

Improved the script in the fix.

SQL6-D0-012900

Updated check content to include a review of system documentation.

Network Infrastructure Policy STIG, Version 10, Release 1**NET0185**

Updated requirement to include IPv6 ULA address space.

NET0198

Updated requirement to severity of CAT II, and expanded the info collected.

NET1622

Updated requirement to replace references to Mission Assurance Categories.

Network SRG, Version 3, Release 0.1**SRG-NET-000371**

Add example in discussion to clarify. Change not needed in subordinate STIGs.

SRG-NET-000522

Removed use for SHA-1 for legacy systems in discussion. Updated document reference.

SRG-NET-000400

Removed use for SHA-1 for legacy systems in discussion. Updated document reference.

SRG-NET-000062

Removed verbiage "is not applicable to VPN devices".

SRG-NET-000570

Removed reference to community strings and updated vulnerability discussion.

SRG-NET-000352

Replaced Commercial Solution for Classified (CSfC) references.

SRG-NET-000565

Replaced Commercial Solution for Classified (CSfC) references.

SRG-NET-000070

Updated the confidentiality modes.

SRG-NET-000525

Updated the confidentiality modes.

SRG-NET-000230

Updated discussion to indicate SHA-2 is needed to protect authenticity.

SRG-NET-000168

Updated discussion document reference, remove sha-1, and updated permitted algorithms.

SRG-NET-000585

Removed requirement.

Oracle 11.2g Database STIG, Version 2, Release 3

O112-BP-024750

Reparenting to SRG-APP-000456-DB-000400.

Oracle Database 12c STIG, Version 2, Release 3

O121-BP-024750

Reparenting to SRG-APP-000456-DB-000400.

Oracle HTTP Server 12.1.3 STIG, Version 2, Release 1

OH12-1X-000167

Corrected typo.

OH12-1X-000282

Corrected typo.

Oracle Linux 6 STIG, Version 2, Release 6

OL6-00-000184

Grouped like syscalls into this requirement.

OL6-00-000185

Grouped like syscalls into this requirement.

OL6-00-000190

Grouped like syscalls into this requirement.

OL6-00-000197

Grouped like syscalls into this requirement.

OL6-00-000202

Grouped like syscalls into this requirement.

OL6-00-000186

Combined requirement with OL6-00-000184.

OL6-00-000187

Combined requirement with OL6-00-000184.

OL6-00-000188

Combined requirement with OL6-00-000185.

OL6-00-000189

Combined requirement with OL6-00-000185.

OL6-00-000192

Combined requirement with OL6-00-000185.

OL6-00-000191

Combined requirement with OL6-00-000190.

OL6-00-000193

Combined requirement with OL6-00-000190.

OL6-00-000194

Combined requirement with OL6-00-000190.

OL6-00-000195

Combined requirement with OL6-00-000190.

OL6-00-000196

Combined requirement with OL6-00-000190.

OL6-00-000538

Added requirement to not allow accounts configured with blank or null passwords.

OL6-00-000030

Updated rule title.

OL6-00-000539

Added requirement to explicitly prevent the bypass of password requirements for privilege escalation.

OL6-00-000540

Added requirement to specify the default "include" directory for the `/etc/sudoers` file.

OL6-00-000536

Updated the finding statement.

OL6-00-000537

Updated the finding statement.

Oracle Linux 7 STIG Benchmark, Version 2, Release 6

OL07-00-030370

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-030410

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-030440

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-030510

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-030820

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-030910

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-030380

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030390

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030400

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030420

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030430

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030450

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030460

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030470

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030480

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030490

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030500

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030520

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030530

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030540

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030550

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030821

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030880

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030890

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030900

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-030920

Removed OVAL content for rule in accordance with rule removal from manual STIG.

OL07-00-010190

Modified OVAL logic logic in accordance with manual STIG update.

OL07-00-010342

Modified OVAL logic to include additional audit logic in accordance with manual STIG update.

OL07-00-010343

Modified OVAL logic to include additional audit logic in accordance with manual STIG update.

OL07-00-010310

Modified OVAL logic logic in accordance with manual STIG update.

Oracle Linux 7 STIG, Version 2, Release 6

OL07-00-030370

Grouped like syscalls into this requirement.

OL07-00-030410

Grouped like syscalls into this requirement.

OL07-00-030440

Grouped like syscalls into this requirement.

OL07-00-030510

Grouped like syscalls into this requirement.

OL07-00-030820

Grouped like syscalls into this requirement.

OL07-00-030910

Grouped like syscalls into this requirement.

OL07-00-030380

Combined requirement with OL07-00-030370.

OL07-00-030390

Combined requirement with OL07-00-030370.

OL07-00-030400

Combined requirement with OL07-00-030370.

OL07-00-030420

Combined requirement with OL07-00-030410.

OL07-00-030430

Combined requirement with OL07-00-030410.

OL07-00-030450

Combined requirement with OL07-00-030440.

OL07-00-030460

Combined requirement with OL07-00-030440.

OL07-00-030470

Combined requirement with OL07-00-030440.

OL07-00-030480

Combined requirement with OL07-00-030440.

OL07-00-030490

Combined requirement with OL07-00-030440.

OL07-00-030500

Combined requirement with OL07-00-030510.

OL07-00-030520

Combined requirement with OL07-00-030510.

OL07-00-030530

Combined requirement with OL07-00-030510.

OL07-00-030540

Combined requirement with OL07-00-030510.

OL07-00-030550

Combined requirement with OL07-00-030510.

OL07-00-030821

Combined requirement with OL07-00-030820.

OL07-00-030880

Combined requirement with OL07-00-030910.

OL07-00-030890

Combined requirement with OL07-00-030910.

OL07-00-030900

Combined requirement with OL07-00-030910.

OL07-00-030920

Combined requirement with OL07-00-030910.

OL07-00-010291

Added requirement to not allow accounts configured with blank or null passwords.

OL07-00-010290

Updated rule title.

OL07-00-010190

Updated check content.

OL07-00-020029

Added requirement for file integrity tool to be installed.

OL07-00-010344

Added requirement to explicitly prevent the bypass of password requirements for privilege escalation.

OL07-00-010339

Added requirement to specify the default "include" directory for the /etc/sudoers file.

OL07-00-010342

Updated the finding statement.

OL07-00-010343

Updated the finding statement.

OL07-00-020023

Updated the finding statement.

OL07-00-010310

Updated discussion, check, and fix content.

OL07-00-040500

Updated check and fix content.

Oracle MySQL 8.0 STIG, Version 1, Release 2

MYS8-00-007200

Updated check to exclude tempdb.

Red Hat Enterprise Linux 7 STIG Benchmark, Version 3, Release 6

RHEL-07-030370

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-030410

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-030440

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-030510

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-030820

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-030910

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-030380

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030390

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030400

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030420

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030430

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030450

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030460

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030470

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030480

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030490

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030500

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030520

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030530

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030540

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030550

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030821

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030880

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030890

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030900

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-030920

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-07-010290

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-010190

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-010342

Updated regular expression for OVAL object.

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-010343

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-010310

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-07-020240

Updated the OVAL to look only for the UMASK parameter value in /etc/login.defs.

RHEL-07-020250

Modified OVAL logic to exclude RHEL 7.7 from compliance.

Red Hat Enterprise Linux 7 STIG, Version 3, Release 6**RHEL-07-030370**

Grouped like syscalls into this requirement.

RHEL-07-030410

Grouped like syscalls into this requirement.

RHEL-07-030440

Grouped like syscalls into this requirement.

RHEL-07-030510

Grouped like syscalls into this requirement.

RHEL-07-030820

Grouped like syscalls into this requirement.

RHEL-07-030910

Grouped like syscalls into this requirement.

RHEL-07-030380

Combined requirement with RHEL-07-030370.

RHEL-07-030390

Combined requirement with RHEL-07-030370.

RHEL-07-030400

Combined requirement with RHEL-07-030370.

RHEL-07-030420

Combined requirement with RHEL-07-030410.

RHEL-07-030430

Combined requirement with RHEL-07-030410.

RHEL-07-030450

Combined requirement with RHEL-07-030440.

RHEL-07-030460

Combined requirement with RHEL-07-030440.

RHEL-07-030470

Combined requirement with RHEL-07-030440.

RHEL-07-030480

Combined requirement with RHEL-07-030440.

RHEL-07-030490

Combined requirement with RHEL-07-030440.

RHEL-07-030500

Combined requirement with RHEL-07-030510.

RHEL-07-030520

Combined requirement with RHEL-07-030510.

RHEL-07-030530

Combined requirement with RHEL-07-030510.

RHEL-07-030540

Combined requirement with RHEL-07-030510.

RHEL-07-030550

Combined requirement with RHEL-07-030510.

RHEL-07-030821

Combined requirement with RHEL-07-030820.

RHEL-07-030880

Combined requirement with RHEL-07-030910.

RHEL-07-030890

Combined requirement with RHEL-07-030910.

RHEL-07-030900

Combined requirement with RHEL-07-030910.

RHEL-07-030920

Combined requirement with RHEL-07-030910.

RHEL-07-010291

Added requirement to not allow accounts configured with blank or null passwords.

RHEL-07-010290

Updated rule title.

RHEL-07-010190

Updated check content.

RHEL-07-020029

Added requirement for file integrity tool to be installed.

RHEL-07-010344

Added requirement to explicitly prevent the bypass of password requirements for privilege escalation.

RHEL-07-010339

Added requirement to specify the default "include" directory for the `/etc/sudoers` file.

RHEL-07-010342

Updated the finding statement.

RHEL-07-010343

Updated the finding statement.

RHEL-07-020023

Updated the finding statement.

RHEL-07-010310

Updated discussion, check, and fix content.

RHEL-07-040500

Updated check and fix content.

Red Hat Enterprise Linux 8 STIG Benchmark, Version 1, Release 4

RHEL-08-030200

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030360

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030361

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030420

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030480

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030490

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030210

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030220

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030230

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030240

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030270

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030380

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030362

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030363

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030364

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030365

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030430

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030440

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030450

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030460

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030470

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030500

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030510

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030520

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030530

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-030540

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-010130

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-020100

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-020041

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-030050

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-010560

Removed OVAL content for rule in accordance with rule removal from manual STIG.

RHEL-08-020220

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-010383

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-010384

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-010294

Modified OVAL logic logic in accordance with manual STIG update.

RHEL-08-040021

Updated regular expression for OVAL object.

RHEL-08-020300

Updated to reflect the setting potentially configured in /etc/pwquality.conf.d/*.conf.

RHEL-08-010000

Modified OVAL logic to exclude RHEL 8.1 from compliance and correct RHEL 8.5 detection.

Red Hat Enterprise Linux 8 STIG, Version 1, Release 5

RHEL-08-040321

Added requirement for multi-user.target.

RHEL-08-030200

Grouped like syscalls into this requirement.

RHEL-08-030360

Grouped like syscalls into this requirement.

RHEL-08-030361

Grouped like syscalls into this requirement.

RHEL-08-030420

Grouped like syscalls into this requirement.

RHEL-08-030480

Grouped like syscalls into this requirement.

RHEL-08-030490

Grouped like syscalls into this requirement.

RHEL-08-030210

Combined requirement with RHEL-08-030200.

RHEL-08-030220

Combined requirement with RHEL-08-030200.

RHEL-08-030230

Combined requirement with RHEL-08-030200.

RHEL-08-030240

Combined requirement with RHEL-08-030200.

RHEL-08-030270

Combined requirement with RHEL-08-030200.

RHEL-08-030380

Combined requirement with RHEL-08-030360.

RHEL-08-030362

Combined requirement with RHEL-08-030361.

RHEL-08-030363

Combined requirement with RHEL-08-030361.

RHEL-08-030364

Combined requirement with RHEL-08-030361.

RHEL-08-030365

Combined requirement with RHEL-08-030361.

RHEL-08-030430

Combined requirement with RHEL-08-030420.

RHEL-08-030440

Combined requirement with RHEL-08-030420.

RHEL-08-030450

Combined requirement with RHEL-08-030420.

RHEL-08-030460

Combined requirement with RHEL-08-030420.

RHEL-08-030470

Combined requirement with RHEL-08-030420.

RHEL-08-030500

Combined requirement with RHEL-08-030480.

RHEL-08-030510

Combined requirement with RHEL-08-030480.

RHEL-08-030520

Combined requirement with RHEL-08-030480.

RHEL-08-030530

Combined requirement with RHEL-08-030490.

RHEL-08-030540

Combined requirement with RHEL-08-030490.

RHEL-08-040320

Updated to split out multi-user.target into a separate requirement.

RHEL-08-010400

Updated check text.

RHEL-08-010121

Added requirement to not allow accounts configured with blank or null passwords.

RHEL-08-010131

Combined requirement with RHEL-08-010130.

RHEL-08-010159

Updated check and fix content.

RHEL-08-010160

Updated check and fix content.

RHEL-08-010130

Updated rule title, check, and fix content.

RHEL-08-040090

Updated fix content.

RHEL-08-010351

Added requirement to have library directories group-owned by root.

RHEL-08-010341

Added requirement to have library directories owned by root.

RHEL-08-010331

Added requirement to set library directories to a mode of 755 or less permissive.

RHEL-08-040020

Updated check and fix content.

RHEL-08-020103

Added requirement for systems below version 8.4 to ensure the password complexity module in the

RHEL-08-020102

Added requirement for systems below version 8.4 to ensure the password complexity module in the system-

RHEL-08-020104

Added requirement for systems version 8.4 and above to ensure the password complexity module is

RHEL-08-020101

Added requirement to ensure the password complexity module is enabled in the system-auth file.

RHEL-08-020100

Updated CCI, rule title, check, and fix content.

RHEL-08-040080

Updated fix content.

RHEL-08-020041

Updated check and fix content.

RHEL-08-010090

Updated fix content.

RHEL-08-010030

Updated check content.

RHEL-08-020140

Updated check content.

RHEL-08-040137

Updated check and fix content.

RHEL-08-030050

Removed requirement. CCI is satisfied by RHEL-08-030060.

RHEL-08-010359

Added requirement for file integrity tool to be installed.

RHEL-08-020221

Added requirement to set password reuse minimum in the system-auth file.

RHEL-08-010560

Removed requirement. Requirement is satisfied by RHEL-08-030181

RHEL-08-010287

Updated check and fix content.

RHEL-08-020220

Updated rule title, check, and fix content.

RHEL-08-030660

Updated check command syntax.

RHEL-08-010385

Added requirement to explicitly prevent the bypass of password requirements for privilege escalation.

RHEL-08-010379

Added requirement to specify the default "include" directory for the `/etc/sudoers` file.

RHEL-08-010383

Updated the finding statement.

RHEL-08-010384

Updated the finding statement.

RHEL-08-010294

Updated check and fix content.

RHEL-08-010572

Updated check command output.

Solaris 11 SPARC STIG Benchmark, Version 2, Release 3**SOL-11.1-070130**

Modified OVAL logic logic in accordance with manual STIG update.

Solaris 11 SPARC STIG, Version 2, Release 6**SOL-11.1-070130**

Updated check command syntax.

Solaris 11 X86 STIG Benchmark, Version 2, Release 3**SOL-11.1-070130**

Modified OVAL logic logic in accordance with manual STIG update.

Solaris 11 x86 STIG, Version 2, Release 6**SOL-11.1-070130**

Updated check command syntax.

SUSE Linux Enterprise Server (SLES) 12 STIG, Version 2, Release 6**SLES-12-020411**

Added a requirement for auditing of `unlink`, `unlinkat`, `rename`, `renameat`, and `rmdir` syscalls.

SLES-12-020370

Grouped like syscalls into this requirement.

SLES-12-020420

Grouped like syscalls into this requirement.

SLES-12-020460

Grouped like syscalls into this requirement.

SLES-12-020490

Grouped like syscalls into this requirement.

SLES-12-020740

Grouped like syscalls into this requirement.

SLES-12-020380

Combined requirement with SLES-12-020370.

SLES-12-020390

Combined requirement with SLES-12-020370.

SLES-12-020400

Combined requirement with SLES-12-020370.

SLES-12-020410

Combined requirement with SLES-12-020370.

SLES-12-020430

Combined requirement with SLES-12-020420.

SLES-12-020440

Combined requirement with SLES-12-020420.

SLES-12-020450

Combined requirement with SLES-12-020420.

SLES-12-020470

Combined requirement with SLES-12-020460.

SLES-12-020480

Combined requirement with SLES-12-020460.

SLES-12-020500

Combined requirement with SLES-12-020490.

SLES-12-020510

Combined requirement with SLES-12-020490.

SLES-12-020520

Combined requirement with SLES-12-020490.

SLES-12-020530

Combined requirement with SLES-12-020490.

SLES-12-020540

Combined requirement with SLES-12-020490.

SLES-12-020750

Combined requirement with SLES-12-020740.

SLES-12-010221

Added requirement to not allow accounts configured with blank or null passwords.

SLES-12-010114

Added requirement to explicitly prevent the bypass of password requirements for privilege escalation.

SLES-12-010109

Added requirement to specify the default "include" directory for the /etc/sudoers file.

SLES-12-010112

Updated the finding statement.

SLES-12-010113

Updated the finding statement.

SUSE Linux Enterprise Server (SLES) 15 STIG, Version 1, Release 5

SLES-15-030150

Grouped like syscalls into this requirement.

SLES-15-030190

Grouped like syscalls into this requirement.

SLES-15-030250

Grouped like syscalls into this requirement.

SLES-15-030290

Grouped like syscalls into this requirement.

SLES-15-030530

Grouped like syscalls into this requirement.

SLES-15-030740

Grouped like syscalls into this requirement.

SLES-15-030160

Combined requirement with SLES-15-030150.

SLES-15-030170

Combined requirement with SLES-15-030150.

SLES-15-030180

Combined requirement with SLES-15-030150.

SLES-15-030320

Combined requirement with SLES-15-030150.

SLES-15-030610

Combined requirement with SLES-15-030150.

SLES-15-030200

Combined requirement with SLES-15-030190.

SLES-15-030210

Combined requirement with SLES-15-030190.

SLES-15-030220

Combined requirement with SLES-15-030190.

SLES-15-030230

Combined requirement with SLES-15-030190.

SLES-15-030240

Combined requirement with SLES-15-030190.

SLES-15-030260

Combined requirement with SLES-15-030250.

SLES-15-030270

Combined requirement with SLES-15-030250.

SLES-15-030280

Combined requirement with SLES-15-030250.

SLES-15-030300

Combined requirement with SLES-15-030290.

SLES-15-030310

Combined requirement with SLES-15-030290.

SLES-15-030540

Combined requirement with SLES-15-030530.

SLES-15-030710

Combined requirement with SLES-15-030740.

SLES-15-030720

Combined requirement with SLES-15-030740.

SLES-15-030730

Combined requirement with SLES-15-030740.

SLES-15-030750

Combined requirement with SLES-15-030740.

SLES-15-020181

Added requirement to not allow accounts configured with blank or null passwords.

SLES-15-020104

Added requirement to explicitly prevent the bypass of password requirements for privilege escalation.

SLES-15-020099

Added requirement to specify the default "include" directory for the /etc/sudoers file.

SLES-15-020102

Updated the finding statement.

SLES-15-020103

Updated the finding statement.

SUSE Linux Enterprise Server 12 STIG Benchmark, Version 2, Release 6

SLES-12-020370

Modified OVAL logic logic in accordance with manual STIG update.

SLES-12-020420

Modified OVAL logic logic in accordance with manual STIG update.

SLES-12-020460

Modified OVAL logic logic in accordance with manual STIG update.

SLES-12-020490

Modified OVAL logic logic in accordance with manual STIG update.

SLES-12-020740

Modified OVAL logic logic in accordance with manual STIG update.

SLES-12-020380

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020390

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020400

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020410

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020430

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020440

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020450

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020470

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020480

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020500

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020510

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020520

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020530

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020540

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-020750

Removed OVAL content for rule in accordance with rule removal from manual STIG.

SLES-12-010112

Modified OVAL logic logic in accordance with manual STIG update.

SLES-12-010113

Modified OVAL logic logic in accordance with manual STIG update.

TANS-CL-000005

Corrected maximum allowable time requirement.

z/OS SRR Scripts, Version 6, Release 52**NA**

RemoveD steps in the Job.

Corrected identifiers for Vul ID and Target ID.

ACF2-ES-000430

New Automation.

ACF2-ES-000590

New Automation.

ACF2-ES-000820

New Automation.

ACF2-ES-000840

New Automation.

ACF2-ES-000860

New Automation.

ACF2-ES-000870

New Automation.

ACF2-ES-000890

New Automation.

ACF2-ES-000900

New Automation.

ACF2-ES-000850

New Automation.

ACF2-ES-000910

New Automation.

ACF2-ES-000990

New Automation.

TSS0-ES-000310

Corrected analysis of prefixed permissions.

ZCA1R020

Added analysis for profile "***" with access of deny.

ZCA1R021

Added analysis for profile "***" with access of deny.