APRIL 2021 MAINTENANCE RELEASE: STIGS TO BE RELEASED

A10 Networks ADC ALG , Version 2, Release 1

AADC-AG-000018

Added change to TLS 1.2.and note about options in the fix text.

Adobe Acrobat Reader DC Classic STIG Benchmark, Version 2, Release 1

NA

Moved the benchmark to sunset in correlation with the manual STIG.

Apple macOS 11 (Big Sur) STIG, Version 1, Release 2

APPL-11-002060

Updated the requirement to allow any applications with a valid digital signature to be installed on the system.

APPL-11-002061

Removed requirement to allow for the documented exception of mission essential unsigned applications.

N/A

Updated the "Restrictions Policy" to remove the configuration reference to APPL-11-002061.

APPL-11-000055

Corrected a typo in the check content.

APPL-11-002005

Corrected a typo in the finding statement.

APPL-11-002032

Corrected a typo in the check content.

APPL-11-002038

Corrected a typo in the check and fix content.

APPL-11-003052

Corrected an incorrect file location in the fix text.

Apple OS X 10.13 STIG, Version 2, Release 3

N/A

Updated the "Security and Privacy Policy" to remove the configuration reference to AOSX-13-000711.

AOSX-13-000710

Updated the requirement to allow any applications with a valid digital signature to be installed on the system.

AOSX-13-000711

Removed requirement to allow for the documented exception of mission essential unsigned applications.

AOSX-13-000057
Corrected a STIG ID issue that caused this requirement to be dropped in a previous release.

Apple OS X 10.14 STIG, Version 2, Release 3

N/A
Updated the "Restrictions Policy" to remove the configuration reference to AOSX-14-002061.

AOSX-14-002060
Updated the requirement to allow any applications with a valid digital signature to be installed on the system.

AOSX-14-002061
Removed requirement to allow for the documented exception of mission essential unsigned applications.

Apple OS X 10.15 STIG, Version 1, Release 4

N/A
Updated the "Restrictions Policy" to remove the configuration reference to AOSX-15-002061.

AOSX-15-002060
Updated the requirement to allow any applications with a valid digital signature to be installed on the system.

AOSX-15-002061
Removed requirement to allow for the documented exception of mission essential unsigned applications.

Apple OS/iPad OS 14 STIG, Version 2, Release 1

AIOS-14-010400
Add text to check to clarify exception.

AIOS-14-009300
Correct typo in check/fix text.

AIOS-14-011400
Correct typo in check/fix text.

Canonical Ubuntu 16.04 LTS STIG Benchmark, Version 2, Release 2

NA
Moved the benchmark to sunset in correlation with the manual STIG.

Canonical Ubuntu 16.04 LTS STIG, Version 2, Release 3

N/A
The operating system is no longer supported under general maintenance support by the vendor and the STIG

UTBU-16-010740
Updated the check command to better isolate interactive users.

UTBU-16-010750
Updated the check command to better isolate interactive users.

UTBU-16-010760
Updated the check command to better isolate interactive users.

UBTU-16-010000
Updated the requirement to allow for documented use of the operating system if extended maintenance

Canonical Ubuntu 18.04 LTS STIG Benchmark, Version 2, Release 2

UBTU-18-010322
Updated OVAL logic to include automation for UBTU-18-010367.

UBTU-18-010387
Updated OVAL logic to include automation for UBTU-18-010355.

UBTU-18-010388
Updated OVAL logic to include automation for UBTU-18-010357.

UBTU-18-010367
Disabled OVAL content for UBTU-18-010367 as it has been merged into UGTU-18-010322.

UBTU-18-010355
Disabled OVAL content for UBTU-18-010355 as it has been merged into UGTU-18-010387.

UBTU-18-010357
Disabled OVAL content for UBTU-18-010357 as it has been merged into UGTU-18-010388.

UBTU-18-010352
Updated OVAL logic changing the target path to /usr/sbin/usermod from /usr/bin/usermod.

Canonical Ubuntu 18.04 LTS STIG, Version 2, Release 3

UBTU-18-010322
Combined with UBTU-18-010367.

UBTU-18-010387
Combined with UBTU-18-010355.

UBTU-18-010321
Combined with UBTU-18-010366.

UBTU-18-010388
Combined with UBTU-18-010357, UBTU-18-010380.

UBTU-18-010367
Removed duplicate requirement.

UBTU-18-010355
Removed duplicate requirement.

UBTU-18-010366
Removed duplicate requirement.

UBTU-18-010357
Removed duplicate requirement.

UBTU-18-010380
Removed duplicate requirement.

UBTU-18-010324
Updated the grep command in the check to use "removexattr".

UBTU-18-010143
Updated the fix command to ignore SGID files.

UBTU-18-010450
Added a rule to require specific ownership of an interactive user's home directory.

UBTU-18-010451
Added a rule to require a specific permission set for an interactive user's home directory.

UBTU-18-010452
Added a rule to require specific group ownership of an interactive user's home directory.

Cisco IOS L2 Switch STIG, Version 2, Release 1

CISC-L2-000160
Corrected configuration example in check and fix content.

Cisco IOS Router NDM STIG, Version 2, Release 2

CISC-ND-000490
Updated vulnerability discussion to allow secure network location for 'break glass' passwords.

CISC-ND-000010
Corrected configuration example in check and fix content.

Cisco IOS Switch NDM STIG, Version 2, Release 2

CISC-ND-000490
Updated vulnerability discussion to allow secure network location for 'break glass' passwords.

Cisco IOS Switch RTR STIG, Version 2, Release 1

CISC-RT-000235
Added requirement to enable IPv4 and IPv6 CEF

CISC-RT-000236
Added requirement to set hop limit to at least 32 for IPv6 stateless auto-configuration deployments.

CISC-RT-000237

Added requirement to prohibit use of IPv6 Site Local addresses.

CISC-RT-000391
Added requirement to suppress IPv6 Router Advertisements at external interfaces.

CISC-RT-000392
Added requirement to drop IPv6 undetermined transport packets.

CISC-RT-000393
Added requirement to drop IPv6 packets with a Routing Header type 0, 1, or 3-255.

CISC-RT-000394
Added requirement to drop IPv6 packets containing a Hop-by-Hop header with invalid option type values.

CISC-RT-000395
Added requirement to drop IPv6 packets containing a Destination Option header with invalid option type

CISC-RT-000396
Added requirement to drop IPv6 packets containing an extension header with the Endpoint Identification

CISC-RT-000397
Added requirement to drop IPv6 packets containing the NSAP address option within Destination Option

CISC-RT-000398
Added requirement to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header

Cisco IOS-XE L2 Switch STIG, Version 2, Release 1

CISC-L2-000160
Corrected configuration example in check and fix content.

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

CISC-ND-000490
Updated vulnerability discussion to allow secure network location for 'break glass' passwords.

CISC-ND-000010
Corrected configuration example in check and fix content.

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

CISC-RT-000080
Updated the check/fix content for correct call-home syntax.

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

CISC-ND-000490
Updated vulnerability discussion to allow secure network location for 'break glass' passwords.

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

CISC-RT-000235

Added requirement to enable IPv4 and IPv6 CEF

CISC-RT-000236
Added requirement to set hop limit to at least 32 for IPv6 stateless auto-configuration deployments.

CISC-RT-000237
Added requirement to prohibit use of IPv6 Site Local addresses.

CISC-RT-000391
Added requirement to suppress IPv6 Router Advertisements at external interfaces.

CISC-RT-000392
Added requirement to drop IPv6 undetermined transport packets.

CISC-RT-000393
Added requirement to drop IPv6 packets with a Routing Header type 0, 1, or 3-255.

CISC-RT-000394
Added requirement to drop IPv6 packets containing a Hop-by-Hop header with invalid option type values.

CISC-RT-000395
Added requirement to drop IPv6 packets containing a Destination Option header with invalid option type

CISC-RT-000396
Added requirement to drop IPv6 packets containing an extension header with the Endpoint Identification

CISC-RT-000397
Added requirement to drop IPv6 packets containing the NSAP address option within Destination Option

CISC-RT-000398
Added requirement to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header

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

CISC-ND-000490
Updated vulnerability discussion to allow secure network location for 'break glass' passwords.

Cisco NS-OX Switch NDM STIG, Version 2, Release 1

CISC-ND-000490
Updated vulnerability discussion to allow secure network location for 'break glass' passwords.

CISC-ND-000150
Updated the check/fix content for correct 15 minute syntax

Cisco NX-OS Switch NDM STIG, Version 2, Release 2

CISC-ND-000140
Corrected configuration example in check and fix content.

Cisco NX-OS Switch RTR STIG, Version 2, Release 1

CISC-RT-000236

Added requirement to set hop limit to at least 32 for IPv6 stateless auto-configuration deployments.

CISC-RT-000237

Added requirement to prohibit use of IPv6 Site Local addresses.

CISC-RT-000391

Added requirement to suppress IPv6 Router Advertisements at external interfaces.

Docker Enterprise 2.x Linux/Unix, Version 2, Release 1

DKER-EE-002110

Modified the check and finding statement in order to add clarity.

DKER-EE-001960

Added exclusion for system containers UCP|DTR|Kube.

Google Chrome Current Windows STIG Benchmark, Version 2, Release 3

DTBC-0006

Updated OVAL logic to match the Google Chrome STIG update.

DTBC-0005

Updated OVAL logic to match the Google Chrome STIG update.

DTBC-0038

Updated OVAL logic to match the Google Chrome STIG update.

Google Chrome STIG, Version 2, Release 3

DTBC-0006

Updated deprecated policy setting in DTBC-0006.

DTBC-0005

Updated deprecated policy setting in DTBC-0005.

DTBC-0038

Updated deprecated policy setting in DTBC-0038.

DTBC-0051

Removed deprecated requirement DTBC-0051.

DTBC-0073

Added TBD to disable Web Bluetooth API

DTBC-0008

Fixed typo in DTBC-0008 check text.

DTBC-0013

Removed deprecated requirement DTBC-0013.

DTBC-0040

Removed deprecated requirement DTBC-0040.

HBSS ePO 5.x Security Technical Implementation Guide, Version 2, Release 3

H20260 - ePO 5x

Removed references to Arcsight under Ports and protocols.

H40180 - ePO 5x

Modified check criteria to clarify dormant account requirement.

H34100 - ePO 5x

Modified check criteria to add Azure environments as not subject to RSD requirements.

H36960 - ePO 5x

Removed references to Arcsight under Ports and protocols.

HBSS McAfee Agent Security Technical Implementation Guide, Version 2, Release 1

H35190

Modified criteria to include use of PA 6.4.3.

HBSS_Distributed_Repository, Version 2, Release 1

N/A

STIG was sunset due to no requirements.

H38100

Removed STIG requirement as no longer necessary.

IBM AIX 7.X STIG, Version 2, Release 2

AIX7-00-002105

Updated "ClientAliveInterval" value to "600". Combined this requirement with AIX7-00-003002.

AIX7-00-003002

Combined requirement with AIX7-00-002105.

IBM zOS ACF2 STIG, Version 8, Release 2

ACF2-OS-000330

Included .jks files when searching.

ACF2-ES-000810

Revised check commands.

ACF2-ES-000820

Revised check commands.

ACF2-ES-000840

Revised check commands.

ACF2-ES-000850
Revised check commands.

ACF2-ES-000860
Revised check commands.

ACF2-ES-000870
Revised check commands.

ACF2-ES-000880
Revised check commands.

ACF2-ES-000890
Revised check commands.

ACF2-ES-000900
Revised check commands.

ACF2-ES-000910
Revised check commands.

ACF2-ES-000920
Added Set Control to Check commands.

ACF2-ES-000940
Added Set Control to Check commands.

ACF2-ES-000950
Added Set Control to Check commands.

ACF2-ES-000960
Added Set Control to Check commands.

ACF2-ES-000990
Revised check commands.

ACF2-US-000180
Adjust Check to all documented justification.

ACF2-ES-000420
Removed. This control is better defined in ACF2-ES-000430

ACF2-ES-000570
Revised control to allow RULELONG where required.

ACF2-ES-000580
Corrected typo in JOBCK.

ACF2-ES-000630
Improved the command in the check.

ACF2-ES-000750
Improved the command in the check.

IBM zOS RACF STIG , Version 8, Release 3

RACF-SH-000060
Include .jks files when searching.

RACF_UT_000030
Correct Check text to match Rule Title

IBM zOS RACF STIG, Version 8, Release 3

RACF-ES-000785
Clarify the minimum Password phrase Length

IBM zOS TSS STIG, Version 8, Release 2

TSS0_ES_000100
Include .jks files when searching.

TSS0-ES_000110
This is a duplicate of TSS0_ES_000100.

JRSS STIG, Version 2, Release 1

JIE-JRSS-005
Modified vulnerability discussion, check and fix.

Juniper SRX SG NDM STIG, Version 2, Release 1

JUSX-DM-000038
Delete JUSX-DM-000038 from the STIG in the next quarterly since it is no longer needed and is redundant and

Juniper SRX SG VPN STIG, Version 2, Release 1

JUSX-VN-000003
Corrected rule title and check content to reflect default value of 28800 seconds which meets this criteria so if

JUSX-VN-000002
Corrected rule title and vulnerability discussion.

JUSX-VN-000022
Corrected to state "If the dead-peer-detection is not configured, this is a finding."

McAfee ENS 10.x Security Technical Implementation Guide, Version 2, Release 3

ENS-EP-000004

Added comment about DISA EMCC signature guide not going to be available until ENS Exploit Prevention is

ENS-FW-000010
Removed requirement as a duplicate of V-230197.

ENS-FW-000001
Added comment about applicability if HIPS still be used.

ENS-FW-000002
Corrected verbiage to reflect the intent of the requirement.
Added comment about applicability if HIPS still be used.

ENS-FW-000003
Added comment about applicability if HIPS still be used.
Modified steps in check criteria.

ENS-FW-000005
Added comment about applicability if HIPS still be used.

ENS-FW-000006
Added comment about applicability if HIPS still be used.

ENS-FW-000007
Added comment about applicability if HIPS still be used.

ENS-FW-000008
Added comment about applicability if HIPS still be used.

ENS-FW-000009
Added comment about applicability if HIPS still be used.
Modified steps in check criteria to select the "Use FTP protocol inspection" option.

ENS-EP-000001
Added comment about applicability if HIPS still be used.
Modified check criteria steps to specify mode to be under Advanced.

ENS-EP-000002
Added comment about applicability if HIPS still be used.

ENS-EP-000003
Added comment about applicability if HIPS still be used.

ENS-CO-000106
Modified check and fix criteria to specify between 50 and 100MB throughout.

ENS-TP-000237
Removing STIG requirement. Default configuration is compliant and sites can configure to their own network's

ENS-CO-000112
Modified check and fix criteria to reflect steps for clarity.

McAfee TIE/DXL Security Technical Implementation Guide , Version 2, Release 2

TIDX-SV-000007
Modified check criteria to allow use of FQDN for ATD.

Microsoft Exchange 2016 Mailbox Server Security Technical Implementation Guide, Version 2, Rele

EX16-MB-000640
Modified check and fix criteria to correctly match requirement.

EX16-MB-002910
Clarified check criteria to use Exchange Management shell instead of PowerShell.

Microsoft IIS 10.0 STIG, Version 2, Release 2

IIST-SV-000205
Altered Check/Fix content in IIST-SV-000205.

IIST-SV-000159
Altered Check/Fix content in IIST-SV-000159.

IIST-SV-000210
Added requirement to remove HTTPAPI Server version from the HTTP Response Header information.

IIST-SV-000215
Added requirement to remove PHP version from the HTTP Response Header information.

IIST-SI-000230
Added NA statement for Splunk.

Microsoft IIS 8.5 STIG, Version 2, Release 2

IISW-SV-000159
Altered Check/Fix content in IISW-SV-000159.

IISW-SV-000153
Altered Check/Fix content in IISW-SV-000153.

IISW-SI-000230
Added NA statement for Splunk IISW-SI-000230.
Added NA statement for Exchange.

IISW-SI-000215
Altered Check/Fix content in IISW-SI-000215.

Microsoft Office 365 ProPlus Security Technical Implementation Guide, Version 2, Release 2

O365-EX-000013

Corrected registry key and setting.

O365-EX-000029
Corrected registry key and setting.

O365-EX-000030
Corrected registry key and setting.

Microsoft SQL Server 2016 Instance STIG, Version 2, Release 3

SQL6-D0-008200
Corrected sentence for configuration navigation .

Microsoft Windows 2012 Server Domain Name System Security Technical Implementation Guide, V

WDNS-AU-000006
Modified check criteria to remove elements of Debug Logging.

Motorola Android 9 STIG, Version 2, Release 1

N/A
Updated the STIG Overview document: changed "Motorola" to "Motorola Solutions" to reflect correct legal

Mozilla Firefox STIG for RHEL Benchmark, Version 5, Release 2

DTBF195
Added OVAL content to the benchmark.

Mozilla Firefox STIG for Windows Benchmark, Version 5, Release 2

DTBF195
Added OVAL content to the benchmark.

Network Device Management SRG, Version 4, Release 1

SRG-APP-000177-NDM-000263
Added PKI account mapping requirement

SRG-APP-000033-NDM-000212
Updated requirement to support AAA broker

SRG-APP-000149-NDM-000247
Added PKI Multifactor requirement

SRG-APP-000175-NDM-000262
Added PKI certificate requirement

Oracle 11.2g Database STIG, Version 2, Release 1

NA
Sunset Oracle 11.2 STIG

O121-C2-002000
Changed STIG_ID to match up with Database SRG.

O112-C2-001600
Removed requirement - Repetitive audit check.

O112-BP-024750
Added requirement that version must be supported by the vendor.

O112-C2-012900
Changed to require integration with an organization-level authentication/access mechanism, and making

O112-C2-013000
Combined with O112-C2-012900.

O112-C2-013100
Combined with O112-C2-012900.

O112-C2-013200
Combined with O112-C2-012900.

O112-C2-001900
Changed STIG_ID to match up with Database SRG.

O112-C2-003000
Changed STIG_ID to match up with Database SRG.

O112-C2-003500
Changed STIG_ID to match up with Database SRG.

O112-C2-003600
Changed STIG_ID to match up with Database SRG.

O112-C2-003700
Changed STIG_ID to match up with Database SRG.

O112-C2-003800
Changed STIG_ID to match up with Database SRG.

O112-C2-003900
Changed STIG_ID to match up with Database SRG.

O112-C2-004000
Changed STIG_ID to match up with Database SRG.

O112-C2-004100
Changed STIG_ID to match up with Database SRG.

O112-C2-004300

Changed STIG_ID to match up with Database SRG.

O112-C2-004400
Changed STIG_ID to match up with Database SRG.

O112-C1-004500
Changed STIG_ID to match up with Database SRG.

O112-OS-004600
Changed STIG_ID to match up with Database SRG.

O112-C2-004900
Changed STIG_ID to match up with Database SRG.

O112-C2-005000
Changed STIG_ID to match up with Database SRG.

O112-C2-006600
Changed STIG_ID to match up with Database SRG.

O112-C2-006700
Changed STIG_ID to match up with Database SRG.

O112-P2-008100
Changed STIG_ID to match up with Database SRG.
Removed requirement - Policy based requirement.

O112-C2-008200
Changed STIG_ID to match up with Database SRG.

O112-C2-008300
Changed STIG_ID to match up with Database SRG.

O112-C2-008900
Removed requirement - Policy based requirement.

O112-C2-009000
Removed requirement - Policy based requirement.

O112-C2-010300
Changed STIG_ID to match up with Database SRG.

O112-C1-011100
Changed STIG_ID to match up with Database SRG.

O112-OS-011200
Changed STIG_ID to match up with Database SRG.

O112-C2-012300
Changed STIG_ID to match up with Database SRG.

O112-C2-012400
Changed STIG_ID to match up with Database SRG.

O112-C2-012500
Changed STIG_ID to match up with Database SRG.

O112-C2-013300
Changed STIG_ID to match up with Database SRG.

O112-C2-013800
Changed STIG_ID to match up with Database SRG.

O112-C2-013900
Changed STIG_ID to match up with Database SRG.

O112-C2-014000
Changed STIG_ID to match up with Database SRG.

O112-C2-014100
Changed STIG_ID to match up with Database SRG.

O112-C2-014200
Changed STIG_ID to match up with Database SRG.

O112-C2-014300
Changed STIG_ID to match up with Database SRG.

O112-C2-014400
Changed STIG_ID to match up with Database SRG.

O112-C2-014500
Changed STIG_ID to match up with Database SRG.

O112-C2-014900
Changed STIG_ID to match up with Database SRG.

O112-C1-015000
Changed STIG_ID to match up with Database SRG.

O112-C2-015100
Changed STIG_ID to match up with Database SRG.

O112-C2-015200

Changed STIG_ID to match up with Database SRG.

O112-C2-016000
Changed STIG_ID to match up with Database SRG.

O112-C2-016100
Changed STIG_ID to match up with Database SRG.

O112-C2-016500
Changed STIG_ID to match up with Database SRG.

O112-C2-016600
Changed STIG_ID to match up with Database SRG.

O112-C2-016700
Changed STIG_ID to match up with Database SRG.

O112-C2-018600
Changed STIG_ID to match up with Database SRG.

O112-C2-019100
Changed STIG_ID to match up with Database SRG.

O112-C2-019600
Changed STIG_ID to match up with Database SRG.

O112-C1-019700
Changed STIG_ID to match up with Database SRG.

O112-C2-020300
Changed STIG_ID to match up with Database SRG.

O112-BP-021200
Changed STIG_ID to match up with Database SRG.

O112-BP-021300
Changed STIG_ID to match up with Database SRG.

O112-BP-021400
Changed STIG_ID to match up with Database SRG.

O112-BP-021500
Changed STIG_ID to match up with Database SRG.

O112-BP-021600
Changed STIG_ID to match up with Database SRG.

O112-BP-021700
Changed STIG_ID to match up with Database SRG.

O112-BP-021900
Changed STIG_ID to match up with Database SRG.

O112-BP-022000
Changed STIG_ID to match up with Database SRG.

O112-BP-022100
Changed STIG_ID to match up with Database SRG.

O112-BP-022200
Changed STIG_ID to match up with Database SRG.

O112-BP-022300
Changed STIG_ID to match up with Database SRG.

O112-BP-022400
Changed STIG_ID to match up with Database SRG.

O112-BP-022500
Changed STIG_ID to match up with Database SRG.

O112-BP-022600
Changed STIG_ID to match up with Database SRG.

O112-BP-022700
Changed STIG_ID to match up with Database SRG.

O112-BP-022800
Changed STIG_ID to match up with Database SRG.

O112-BP-022900
Changed STIG_ID to match up with Database SRG.

O112-BP-023000
Changed STIG_ID to match up with Database SRG.

O112-BP-023100
Changed STIG_ID to match up with Database SRG.

O112-BP-023200
Changed STIG_ID to match up with Database SRG.

O112-BP-023300
Changed STIG_ID to match up with Database SRG.

O112-BP-023600
Changed STIG_ID to match up with Database SRG.

O112-BP-023700
Changed STIG_ID to match up with Database SRG.

O112-BP-023800
Changed STIG_ID to match up with Database SRG.

O112-BP-023900
Changed STIG_ID to match up with Database SRG.

O112-BP-024000
Changed STIG_ID to match up with Database SRG.

O112-BP-024100
Changed STIG_ID to match up with Database SRG.

O112-BP-024200
Changed STIG_ID to match up with Database SRG.

O112-BP-025400
Changed STIG_ID to match up with Database SRG.

O112-BP-025500
Changed STIG_ID to match up with Database SRG.

O112-BP-025600
Changed STIG_ID to match up with Database SRG.

O112-BP-025800
Changed STIG_ID to match up with Database SRG.

O112-BP-026200
Changed STIG_ID to match up with Database SRG.

O112-BP-026300
Changed STIG_ID to match up with Database SRG.

O112-BP-026400
Changed STIG_ID to match up with Database SRG.

O112-BP-026500
Changed STIG_ID to match up with Database SRG.

O112-BP-026600

Changed STIG_ID to match up with Database SRG.

O112-BP-025101
Changed STIG_ID to match up with Database SRG.

O112-C2-002200
Removed requirement - covered in O112-C2-006800.

O112-C2-002300
Removed requirement - covered in O112-C2-006800.

O112-C2-002400
Removed requirement - covered in O112-C2-006800.

O112-C2-002500
Removed requirement - covered in O112-C2-006800.

O112-C3-003300
Removed requirement - CCI has been withdrawn.

O112-C2-003400
Removed requirement - CCI has been withdrawn.

O112-C2-004200
Removed requirement - Covered somewhere else.

O112-C2-004210
Removed requirement - Duplicate.

O112-N2-004701
Removed requirement - generic and policy based. Not adding value.

O112-C2-005600
Removed requirement - covered in O112-N2-008601.

O112-C2-005700
Removed requirement - covered in O112-N2-008601.

O112-C2-008500
Removed requirement - covered in SRG-APP-000360-DB-000320.

O112-C3-008700
Removed requirement - covered in SRG-APP-000353-DB-000324.

O112-C3-008800
Removed requirement - covered in SRG-APP-000353-DB-000324.

O112-C2-010000
Removed requirement - Off loading to a central log server covers this.

O112-C2-010100
Removed requirement - Combined with Audit tools and don't need to encryption unless the data requires it.

O112-C2-010200
Removed requirement - Combined with Audit tools and don't need to encryption unless the data requires it.

O112-C2-011400
Removed requirement - Policy based and vague.

O112-C2-012000
Removed requirement - Redundant requirement.

O112-C2-012200
Removed requirement - User information is included in database backups.

O112-C2-012600
Removed requirement - Not needed in a database STIG.

O112-P2-012700
Removed requirement - Redundant requirement.

O112-C2-013600
Removed requirement - Checks for the sqlnet.ora settings are in several other reqs.

O112-C2-013700
Removed requirement - Checks for the sqlnet.ora settings are in several other reqs.

O112-C2-016300
Removed requirement - CCI has been withdrawn.

O112-C2-016400
Removed requirement - CCI has been withdrawn.

O112-C2-017100
Removed requirement - Vague and policy based.

O112-P2-017400
Removed requirement - Non specific vendor documentation check.

O112-C2-018800
Removed requirement - Monitoring already covered in SRG-APP-000133-DB-000179 plus this is something

O112-C3-019200
Removed requirement - Redundant.

O112-C3-019300
Removed requirement - Redundant.

O112-C3-019400
Removed requirement - Redundant - already checking session limits.

O112-C2-019800
Removed requirement - Vague - No value added.

O112-C2-020400
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O112-C2-020500
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O112-C2-020600
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O112-C2-020700
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O112-BP-021100
Removed requirement - Policy based requirement.

O112-BP-023400
Removed requirement - Policy based requirement.

O112-BP-023500
Removed requirement - Policy based requirement.

O112-BP-024300
Removed requirement - Policy based requirement.

O112-BP-024400
Removed requirement - Policy based requirement - no clear configuration settings.

O112-BP-024500
Removed requirement - Policy based requirement.

O112-BP-024600
Removed requirement - Policy based requirement.

O112-BP-024700
Removed requirement - Policy based requirement.

O112-BP-024800

Removed requirement - Policy based requirement.

O112-BP-024900
Removed requirement - Policy based requirement.

O112-BP-025200
Removed requirement - Policy based requirement - no clear configuration settings.

O112-BP-025300
Removed requirement - Policy based requirement - no clear configuration settings.

O112-BP-026000
Removed requirement - Policy based requirement - no clear configuration settings.

O112-BP-026100
Removed requirement - Policy based requirement - Keys are well covered in other checks.

O112-C2-018400
Removed requirement - Policy based requirement.

O112-C2-017700
Removed requirement - Policy based requirement.

O112-C2-005200
Removed requirement - Policy based requirement.

O112-C3-020200
Removed requirement - Policy based requirement.

O112-C2-001700
Changed STIG_ID to match up with Database SRG.

Oracle Database 12c STIG, Version 2, Release 1

NA
Corrected revision history.

O121-C2-012900
Changed to require integration with an organization-level authentication/access mechanism, and making

O121-C2-013000
Combined with O121-C2-012900.

O121-C2-013100
Combined with O121-C2-012900.

O121-C2-013200
Combined with O121-C2-012900.

O121-BP-022500
Updated administrative privileges list.
Changed STIG_ID to match up with Database SRG.

O121-BP-022300
Updated administrative privileges list.
Changed STIG_ID to match up with Database SRG.

O121-BP-022600
Updated administrative privileges list.
Changed STIG_ID to match up with Database SRG.

O121-C2-011600
Updated query in check content.

O121-C2-001700
Changed STIG_ID to match up with Database SRG.

O121-C2-001900
Changed STIG_ID to match up with Database SRG.

O121-C2-002000
Changed STIG_ID to match up with Database SRG.

O121-C2-003000
Changed STIG_ID to match up with Database SRG.

O121-C2-003500
Changed STIG_ID to match up with Database SRG.

O121-C2-003600
Changed STIG_ID to match up with Database SRG.

O121-C2-003700
Changed STIG_ID to match up with Database SRG.

O121-C2-003800
Changed STIG_ID to match up with Database SRG.

O121-C2-003900
Changed STIG_ID to match up with Database SRG.

O121-C2-004000
Changed STIG_ID to match up with Database SRG.

O121-C2-004100

Changed STIG_ID to match up with Database SRG.

O121-C2-004300
Changed STIG_ID to match up with Database SRG.

O121-C2-004400
Changed STIG_ID to match up with Database SRG.

O121-C1-004500
Changed STIG_ID to match up with Database SRG.

O121-OS-004600
Changed STIG_ID to match up with Database SRG.

O121-C2-004900
Changed STIG_ID to match up with Database SRG.

O121-C2-005000
Changed STIG_ID to match up with Database SRG.

O121-C2-006600
Changed STIG_ID to match up with Database SRG.

O121-C2-006700
Changed STIG_ID to match up with Database SRG.

O121-C2-008200
Changed STIG_ID to match up with Database SRG.

O121-C2-008300
Changed STIG_ID to match up with Database SRG.

O121-C2-008900
Remove requirement - Policy based requirement

O121-C2-009000
Remove requirement - Redundant requirement

O121-C2-010300
Changed STIG_ID to match up with Database SRG.

O121-C1-011100
Changed STIG_ID to match up with Database SRG.

O121-OS-011200
Changed STIG_ID to match up with Database SRG.

O121-C2-012300
Changed STIG_ID to match up with Database SRG.

O121-C2-012400
Changed STIG_ID to match up with Database SRG.

O121-C2-012500
Changed STIG_ID to match up with Database SRG.

O121-C2-013300
Changed STIG_ID to match up with Database SRG.

O121-C2-013800
Changed STIG_ID to match up with Database SRG.

O121-C2-013900
Changed STIG_ID to match up with Database SRG.

O121-C2-014000
Changed STIG_ID to match up with Database SRG.

O121-C2-014100
Changed STIG_ID to match up with Database SRG.

O121-C2-014200
Changed STIG_ID to match up with Database SRG.

O121-C2-014300
Changed STIG_ID to match up with Database SRG.

O121-C2-014400
Changed STIG_ID to match up with Database SRG.

O121-C2-014500
Changed STIG_ID to match up with Database SRG.

O121-C2-014900
Changed STIG_ID to match up with Database SRG.

O121-C1-015000
Changed STIG_ID to match up with Database SRG.

O121-C2-015100
Changed STIG_ID to match up with Database SRG.

O121-C2-015200
Changed STIG_ID to match up with Database SRG.

O121-C2-016000
Changed STIG_ID to match up with Database SRG.

O121-C2-016100
Changed STIG_ID to match up with Database SRG.

O121-C2-016500
Changed STIG_ID to match up with Database SRG.

O121-C2-016600
Changed STIG_ID to match up with Database SRG.

O121-C2-016700
Changed STIG_ID to match up with Database SRG.

O121-C2-018600
Changed STIG_ID to match up with Database SRG.

O121-C2-019100
Changed STIG_ID to match up with Database SRG.

O121-C2-019600
Changed STIG_ID to match up with Database SRG.

O121-C1-019700
Changed STIG_ID to match up with Database SRG.

O121-C2-020300
Changed STIG_ID to match up with Database SRG.

O121-BP-021200
Changed STIG_ID to match up with Database SRG.

O121-BP-021300
Changed STIG_ID to match up with Database SRG.

O121-BP-021400
Changed STIG_ID to match up with Database SRG.

O121-BP-021500
Changed STIG_ID to match up with Database SRG.

O121-BP-021600
Changed STIG_ID to match up with Database SRG.

O121-BP-021700

Changed STIG_ID to match up with Database SRG.

O121-BP-021900
Changed STIG_ID to match up with Database SRG.

O121-BP-022000
Changed STIG_ID to match up with Database SRG.

O121-BP-022100
Changed STIG_ID to match up with Database SRG.

O121-BP-022200
Changed STIG_ID to match up with Database SRG.

O121-BP-022400
Changed STIG_ID to match up with Database SRG.

O121-BP-022700
Changed STIG_ID to match up with Database SRG.

O121-BP-022800
Changed STIG_ID to match up with Database SRG.

O121-BP-022900
Changed STIG_ID to match up with Database SRG.

O121-BP-023000
Changed STIG_ID to match up with Database SRG.

O121-BP-023100
Changed STIG_ID to match up with Database SRG.

O121-BP-023200
Changed STIG_ID to match up with Database SRG.

O121-BP-023300
Changed STIG_ID to match up with Database SRG.

O121-BP-023600
Changed STIG_ID to match up with Database SRG.

O121-BP-023700
Changed STIG_ID to match up with Database SRG.

O121-BP-023800
Changed STIG_ID to match up with Database SRG.

O121-BP-023900
Changed STIG_ID to match up with Database SRG.

O121-BP-024000
Changed STIG_ID to match up with Database SRG.

O121-BP-024100
Changed STIG_ID to match up with Database SRG.

O121-BP-024200
Changed STIG_ID to match up with Database SRG.

O121-BP-025400
Changed STIG_ID to match up with Database SRG.

O121-BP-025500
Changed STIG_ID to match up with Database SRG.

O121-BP-025600
Changed STIG_ID to match up with Database SRG.

O121-BP-025800
Changed STIG_ID to match up with Database SRG.

O121-BP-026200
Changed STIG_ID to match up with Database SRG.

O121-BP-026300
Changed STIG_ID to match up with Database SRG.

O121-BP-026400
Changed STIG_ID to match up with Database SRG.

O121-BP-026500
Changed STIG_ID to match up with Database SRG.

O121-BP-026600
Changed STIG_ID to match up with Database SRG.

O121-BP-025100
Changed STIG_ID to match up with Database SRG.

O121-BP-025101
Changed STIG_ID to match up with Database SRG.

O112-C2-001600
Removed requirement - Repetitive audit check.

O121-C2-002200
Removed requirement - covered in O121-C2-006800.

O121-C2-002300
Removed requirement - covered in O121-C2-006800.

O121-C2-002400
Removed requirement - covered in O121-C2-006800.

O121-C2-002500
Removed requirement - covered in O121-C2-006800.

O121-C3-003300
Removed requirement - CCI has been withdrawn.

O121-C2-003400
Removed requirement - CCI has been withdrawn.

O121-C2-004200
Removed requirement - Covered somewhere else.

O121-C2-004210
Removed requirement - Duplicate.

O121-N2-004701
Removed requirement - generic and policy based. Not adding value.

O121-C2-005600
Removed requirement - covered in O121-N2-008601.

O121-C3-008700
Removed requirement - covered in SRG-APP-000353-DB-000324.

O121-C3-008800
Removed requirement - covered in SRG-APP-000353-DB-000324.

O121-C2-010000
Removed requirement - Off loading to a central log server covers this.

O121-C2-010100
Removed requirement - Combined with Audit tools and don't need to encryption unless the data requires it.

O121-C2-010200
Removed requirement - Combined with Audit tools and don't need to encryption unless the data requires it.

O121-C2-011400

Removed requirement - Policy based and vague.

O121-C2-012000
Removed requirement - Redundant requirement.

O121-C2-012200
Removed requirement - User information is included in database backups.

O121-C2-012600
Removed requirement - Not needed in a database STIG.

O121-P2-012700
Removed requirement - Redundant requirement.

O121-C2-013600
Removed requirement - Checks for the sqlnet.ora settings are in several other reqs.

O121-C2-013700
Removed requirement - Checks for the sqlnet.ora settings are in several other reqs.

O121-C2-016300
Removed requirement - CCI has been withdrawn.

O121-C2-016400
Removed requirement - CCI has been withdrawn.

O121-C2-017100
Removed requirement - Vague and policy based.

O121-P2-017400
Removed requirement - Non specific vendor documentation check.

O121-C2-018800
Removed requirement - Monitoring already covered in SRG-APP-000133-DB-000179 plus this is something

O121-C3-019200
Removed requirement - Redundant

O121-C3-019300
Removed requirement - Redundant

O121-C3-019400
Removed requirement - Redundant - already checking session limits

O121-C2-019800
Removed requirement - Vague - No value added

O121-C2-020400
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O121-C2-020500
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O121-C2-020600
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O121-C2-020700
Removed requirement - Redundant to audit requirements. As more account activity occurs at the org level,

O121-BP-021100
Removed requirement - Policy Based.

O121-BP-023400
Removed requirement - Policy based requirement.

O121-BP-023500
Removed requirement - Policy based requirement.

O121-BP-024300
Removed requirement - Policy based requirement - no clear configuration settings.

O121-BP-024400
Removed requirement - Policy based requirement - no clear configuration settings.

O121-BP-024500
Removed requirement - Policy based requirement.

O121-BP-024600
Removed requirement - Policy based requirement.

O121-BP-024700
Removed requirement - Policy based requirement.

O121-BP-024800
Removed requirement - Policy based requirement.

O121-BP-024900
Removed requirement - Policy based requirement.

O121-BP-025200
Removed requirement - Policy based requirement - no clear configuration settings.

O121-BP-025300
Removed requirement - Policy based requirement - no clear configuration settings.

O121-BP-026000
Removed requirement - Policy based requirement - no clear configuration settings.

O121-BP-026100
Removed requirement - Policy based requirement - Keys are well covered in other checks.

O121-C2-015501
Changed to DoD Approved certificates.

O121-C2-007600
Clarified standard vs unified audit checks.

O121-BP-024750
Added requirement that version must be supported by the vendor.

Oracle Linux 6 STIG, Version 2, Release 3

OL6-00-000537
Added requirement to require re-authentication when using sudo.

OL6-00-000536
Added requirement to invoke the user's password when using sudo.

OL6-00-000535
Added requirement to restrict privilege elevation to authorized personnel.

OL6-00-000071
Updated script syntax.

Oracle Linux 7 STIG Benchmark, Version 2, Release 3

OL07-00-040400
Updated OVAL logic to remove inclusion of OL07-00-021350 OVAL logic.

OL07-00-040100
Updated OVAL logic to remove inclusion of OL07-00-021350 OVAL logic.

Oracle Linux 7 STIG, Version 2, Release 3

OL07-00-010010
Updated the command in the Check Content.

OL07-00-010343
Added requirement to require re-authentication when using sudo.

OL07-00-010342
Added requirement to invoke the user's password when using sudo.

OL07-00-010341

Added requirement to restrict privilege elevation to authorized personnel.

OL07-00-040160
Updated time designation and script syntax.

OL07-00-040730
Updated Fix content.

Oracle WebLogic Server 12c, Version 2, Release 1

WBLC-03-000128
DoD ports and protocols web site at https://cyber.mil/ppsm.

WBLC-01-000014
DoD ports and protocols web site at https://cyber.mil/ppsm.

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

RHEL-07-010010
Updated the command in the Check Content.

RHEL-07-010343
Added requirement to require re-authentication when using sudo.

RHEL-07-010342
Added requirement to invoke the user's password when using sudo.

RHEL-07-010341
Added requirement to restrict privilege elevation to authorized personnel.

RHEL-07-040160
Updated script syntax.

RHEL-07-040730
Updated Fix content.

Red Hat Enterprise Linux 8 STIG, Version 1, Release 2

RHEL-08-040060
Removed this requirement as the version of openssh that ships with RHEL 8 does not support SSHv1.

RHEL-08-040003
Merged with RHEL-08-040370.

RHEL-08-040370
Updated CCI mapping.

RHEL-08-010830
Updated Rule Title and Vulnerability Discussion.

RHEL-08-010384
Added requirement to require re-authentication when using sudo.

RHEL-08-010383
Added requirement to invoke the user's password when using sudo.

RHEL-08-010382
Added requirement to restrict privilege elevation to authorized personnel.

RHEL-08-040320
Updated Fix content.

RHEL-08-010161
Updated Check content.

RHEL-08-010162
Updated Check content with a Not Applicable statement.

RHEL-08-010163
Added requirement to remove older versions of the krb5-server package.

RHEL-08-020020
Updated Vulnerability Discussion and Check content.

RHEL-08-020022
Updated Vulnerability Discussion and Check content.

RHEL-08-020060
Updated Vulnerability Discussion and Check content.

RHEL-08-040171
Updated Check content with a Not Applicable statement.

RHEL-08-010290
Updated Check content.

RHEL-08-010291
Updated Check content.

RHEL-08-030180
Updated Check and Fix content.

RHEL-08-020200
Fixed typo in Check content

RHEL 6 STIG Benchmark, Version 2, Release 1

NA

Moved the benchmark to sunset in correlation with the manual STIG.

RHEL 7 STIG Benchmark, Version 3, Release 3

RHEL-07-040110

Updated OVAL logic to remove inclusion of RHEL-07-021350 OVAL logic.

RHEL-07-040400

Updated OVAL logic to remove inclusion of RHEL-07-021350 OVAL logic.

Router SRG, Version 4, Release 2

SRG-NET-000364-RTR-000110

remove IPv6 link-local prefix from Bogon list

SRG-NET-000362-RTR-000123

Correct CCI

SLES 12 STIG Benchmark, Version 2, Release 3

SLES-12-010380

Updated OVAL logic to match the SLES12 STIG update.

SLES-12-010430

Update the OVAL to match the SLES12 STIG update.

Solaris 11 SPARC STIG, Version 2, Release 3

SOL-11.1-040010

Updated Check commands

SOL-11.1-030055

Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050150

Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050160

Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050170

Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050180

Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050190

Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050240

Updated Vulnerability Discussion, Check, Fix, and CCI mappings

SOL-11.1-050270
Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050290
Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050320
Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050330
Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050350
Removed requirement and combined with SOL-11.1-050240

SOL-11.1-050360
Removed requirement and combined with SOL-11.1-050240

Solaris 11 x86 STIG, Version 2, Release 3

SOL-11.1-040010
Updated Check commands.

SOL-11.1-030055
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050150
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050160
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050170
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050180
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050190
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050240
Updated Vulnerability Discussion, Check, Fix, and CCI mappings.

SOL-11.1-050270
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050290
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050320
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050330
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050350
Removed requirement and combined with SOL-11.1-050240.

SOL-11.1-050360
Removed requirement and combined with SOL-11.1-050240.

Splunk Enterprise for Windows 7.x STIG, Version 2, Release 2

SPLK-CL-000020
Updated check text to add "Not Applicable" when web interface is disabled and using a deployment server for

SPLK-CL-000045
Updated check text to add "Not Applicable" when web interface is disabled and using a deployment server for

SPLK-CL-000080
Updated check text to add "Not Applicable" when web interface is disabled and using a deployment server for

SRRAUDIT Dialog Management Document, Version 6, Release 49

NA
Changed process on how information is collected.

Suse Linux Enterprise Server (SLES) 12 STIG, Version 2, Release 3

SLES-12-010710
Updated command syntax

SLES-12-030151
Updated Rule Title and Vulnerability Discussion

SLES-12-010113
Added requirement to require re-authentication when using sudo

SLES-12-010112
Added requirement to invoke the user's password when using sudo

SLES-12-010111
Added requirement to restrict privilege elevation to authorized personnel

SLES-12-010040
Updated Check and Fix content

SLES-12-010050
Updated command syntax and added a Not Applicable statement

SLES-12-010080
Updated Check content and command syntax

SLES-12-010110
Updated Check content

SLES-12-010210
Updated Check and Fix content

SLES-12-010220
Updated Fix content

SLES-12-010260
Updated command syntax and verbiage throughout

SLES-12-010270
Updated command syntax and verbiage throughout

SLES-12-010280
Updated Check and Fix content

SLES-12-010290
Updated Check and Fix content

SLES-12-010380
Updated Check and Fix content

SLES-12-010390
Updated Check content

SLES-12-010520
Updated Check content

SLES-12-010530
Updated Check content

SLES-12-010550
Updated Check and Fix content

SLES-12-010600
Updated Check and Fix content

SLES-12-010610

Updated Check and Fix content

SLES-12-010611
Updated Check and Fix content

SLES-12-010631
Added requirement to limit account capabilities

SLES-12-010780
Updated Check and Fix content

SLES-12-010871
Added requirement to set permissions on system library files

SLES-12-010872
Added requirement to set permissions on system library directories

SLES-12-010873
Added requirement to set the owner of system library files

SLES-12-010874
Added requirement to set the owner of system library directories

SLES-12-010875
Added requirement to set the group-owner of system library files

SLES-12-010876
Added requirement to set the group-owner of system library directories

SLES-12-010877
Added requirement to set permissions on system commands

SLES-12-010878
Added requirement to set permissions on system command directories

SLES-12-010879
Added requirement to set the owner of system commands

SLES-12-010880
Removed requirement

SLES-12-010881
Added requirement to set the owner of system command directories

SLES-12-010882
Added requirement to set the group-owner of system commands

SLES-12-010883
Added requirement to set the group-owner of system command directories

SLES-12-010890
Updated Check and Fix content

SLES-12-010910
Updated Check and Fix content

SLES-12-020050
Updated Check and Fix content

SLES-12-020130
Updated Check and Fix content

SLES-12-020199
Updated command syntax and Rule Title typo

SLES-12-030010
Removed requirement and combined with SLES-12-030011

SLES-12-030011
Added requirement to remove vsftpd package

SLES-12-030210
Updated Check and Fix content

SLES-12-030220
Updated Check and Fix content

SLES-12-030300
Updated Check content

SLES-12-030310
Updated Check and Fix content

SLES-12-030320
Updated Check content

SLES-12-030330
Updated Check content

SLES-12-030362
Added requirement to prevent forwarding of IPV6 source-routed packets

SLES-12-030363
Added requirement to prevent acceptance of IPV6 ICMP redirect messages

SLES-12-030364
Added requirement to prevent IPV6 packet forwarding

SLES-12-030365
Added requirement to set default IPV6 packet forwarding behavior

SLES-12-030430
Updated Rule Title, Check and Fix content

SLES-12-030530
Updated Check content

Suse Linux Enterprise Server (SLES) 15 STIG, Version 1, Release 2

SLES-15-040270
Removed this requirement as the version of openssh that ships with SLES 15 does not support SSHv2.

Virtual Private Network (VPN) SRG, Version 2, Release 3

SRG-NET-000019-VPN-000040
Changed finding statement to read:

If the IPsec VPN Gateway does not use Encapsulating Security Payload (ESP) in tunnel mode for establishing secured paths to transport traffic between the organizations sites or between a gateway and remote end-

z/OS ICSF for ACF2 STIG , Version 6, Release 6

ZICS0040
Revise requirement for the FAIL option for FIPSMODE.

z/OS ICSF for RACF STIG , Version 6, Release 6

ZICS0040
Revise requirement for the FAIL option for FIPSMODE.

z/OS ICSF for TSS STIG , Version 6, Release 6

ZICS0040
Revise requirement for the FAIL option for FIPSMODE.

z/OS SRR Scripts STIG Instruction, Version 6, Release 49

NA
Changes made to initialize a variable

z/OS SRR Scripts, Version 6, Release 49

ZSMTA001
Changed process on how information is collected.

ZSMTR001
Changed process on how information is collected.

ZSMTT001
Changed process on how information is collected.

ACF2-OS-000210
Provide automation for vulnerability.

RACF-OS-000010
Provide automation for vulnerability.

TSS0-OS-000350
Provide automation for vulnerability.

ACF2-OS-000140
Provide automation for vulnerability.

RACF-OS-000170
Provide automation for vulnerability.

TSS0-OS-000020
Provide automation for vulnerability.

ACF2-OS-000130
Provide automation for vulnerability.

RACF-OS-000160
Provide automation for vulnerability.

TSS0-OS-000060
Provide automation for vulnerability.