OCTOBER 2020 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Release Date: October 23, 2020

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

ARDC-CL-000340

ARDC-CL-000340 - Upgraded to CAT I requirement to sunset STIG.

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

NA

Repackaged benchmark to include updated STIG IDs.

Adobe Professional DC Classic STIG, Version 2, Release 1

AADC-CL-001075

AADC-CL-001075 - Upgraded to CAT I requirement to sunset STIG.

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

AS24-U1-000650

AS24-U1-000650 - Clarified vulnerability discussion, added an example to the check, and corrected fix verbiage with a required value.

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

AS24-WI-000640

AS24-WI-000640 - Corrected value for SessionMaxAge directive.

Apache Tomcat Application Server 9 STIG, Version 2, Release 1

TCAT-AS-000030

TCAT-AS-000030 - Updated HSTS instructions in fix and deleted URL references in discussion.

Apple OS X 10.13 STIG, Version 2, Release 1

AOSX-13-000520

AOSX-13-000520 - Upgraded the severity of this requirement to a CAT I.

AOSX-13-000561

AOSX-13-000561 - Updated the check content to ensure that the iCloud preference pane was disabled.

Apple OS X 10.14 (Mojave) STIG, Version 2, Release 1

AOSX-14-000032

AOSX-14-000032 - Updated the requirement to allow for multiple FileVault Users. Updated the CCI to CCI-002143.

AOSX-14-002031

AOSX-14-002031 - Upgraded the severity of this requirement to a CAT I.

AOSX-14-002043

AOSX-14-002043 - Updated the check content to ensure that the iCloud preference pane was disabled.

AOSX-14-005051

AOSX-14-005051 - Removed requirement; it is based on an obsolete GPOS SRG requirement and is no longer necessary.

Application Core SRG, Version 3, Release 0.1

SRG-APP-000416

SRG-APP-000416 - Removed requirement. This is a duplicate of Vul ID: V-80975.

Application Security and Development STIG, Version 5, Release 1

APSC-DV-000940

APSC-DV-000940 - Corrected check content: The word reestablishing was missing an "h".

APSC-DV-001620

APSC-DV-001620 - Corrected TLS version reference. Changed TLSV1.1 to TLSV1.2 or higher.

APSC-DV-001630

APSC-DV-001630 - Corrected TLS version reference. Changed TLSV1.1 to TLSV1.2 or higher.

APSC-DV-000610

APSC-DV-000610 - Removed requirement based on SRG-APP-000353 removal.

Application Server SRG, Version 3, Release 1

SRG-APP-000142-AS-000014

SRG-APP-000142-AS-000014 - Corrected URL pointing to PPSM website.

SRG-APP-000353-AS-000235

SRG-APP-000353-AS-000235 - Requirement removed from SRG; not applicable.

Canonical Ubuntu 16.04 LTS STIG, Version 2, Release 1

UBTU-16-030900

UBTU-16-030900 - Updated the requirement to use CCI-001241.

UBTU-16-030910

UBTU-16-030910 - Updated the requirement to use CCI-001240.

Canonical Ubuntu 16.04 STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

Canonical Ubuntu 18.04 LTS STIG, Version 2, Release 1

UBTU-18-010033

UBTU-18-010033 - Combined requirement with UBTU-18-010039.

UBTU-18-010039

UBTU-18-010039 - Combined requirement with UBTU-18-010033.

UBTU-18-010116

UBTU-18-010116 - Added "enforce_for_root" to the requirement.

UBTU-18-010134

UBTU-18-010134 - Corrected a typo in the fix text.

UBTU-18-010315

UBTU-18-010315 - Updated the example output in the check to match the OS output.

UBTU-18-010328

UBTU-18-010328 - Updated the example output in the check to match the OS output.

UBTU-18-010335

UBTU-18-010335 - Combined requirement with UBTU-18-010382.

UBTU-18-010336

UBTU-18-010336 - Combined requirement with UBTU-18-010383.

UBTU-18-010337

UBTU-18-010337 - Combined requirement with UBTU-18-010384.

UBTU-18-010379

UBTU-18-010379 - Corrected a typo in the check and fix text.

UBTU-18-010380

UBTU-18-010380 - Corrected a typo in the check and fix text.

UBTU-18-010382

UBTU-18-010382 - Combined UBTU-18-010335 with this requirement.

UBTU-18-010383

UBTU-18-010383 - Combined UBTU-18-010336 with this requirement.

UBTU-18-010384

UBTU-18-010384 - Combined UBTU-18-010337 with this requirement.

UBTU-18-010405

UBTU-18-010405 - Combined requirement with UBTU-18-010416.

UBTU-18-010416

UBTU-18-010416 - Combined UBTU-18-010405 with this requirement.

UBTU-18-010507

UBTU-18-010507 - Combined UBTU-18-010520 with this requirement.

UBTU-18-010514

UBTU-18-010514 - Updated the check and fix to better fit the security function of the requirement.

UBTU-18-010520

UBTU-18-010520 - Combined requirement with UBTU-18-010507.

Cisco IOS Router NDM STIG, Version 2, Release 1

CISC-ND-000140

CISC-ND-000140 - Updated check and fix to include log-input on deny statement.

Cisco IOS Router RTR STIG, Version 2, Release 1

CISC-RT-000020

CISC-RT-000020 - Updated vulnerability discussion to provide clarification of the requirement.

CISC-RT-000080

CISC-RT-000080 - Updated check to provide clarification of the requirement.

CISC-RT-000235

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

CISC-RT-000236

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

CISC-RT-000237

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

CISC-RT-000391

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

CISC-RT-000392

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

CISC-RT-000393

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

CISC-RT-000394

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

CISC-RT-000395

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

CISC-RT-000396

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

CISC-RT-000397

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

CISC-RT-000398

CISC-RT-000398 - Added requirement to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type.

Cisco IOS Switch NDM STIG, Version 2, Release 1

CISC-ND-000140

CISC-ND-000140 - Updated check and fix to include log-input on deny statement.

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

CISC-ND-000140

CISC-ND-000140 - Updated check and fix to include log-input on deny statement.

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

CISC-RT-000020

CISC-RT-000020 - Updated vulnerability discussion to provide clarification of the requirement.

CISC-RT-000080

CISC-RT-000080 - Updated check to provide clarification of the requirement.

CISC-RT-000235

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

CISC-RT-000236

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

CISC-RT-000237

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

CISC-RT-000391

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

CISC-RT-000392

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

CISC-RT-000393

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

CISC-RT-000394

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

CISC-RT-000395

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

CISC-RT-000396

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

CISC-RT-000397

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

CISC-RT-000398

CISC-RT-000398 - Added requirement to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type.

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

CISC-ND-000140

CISC-ND-000140 - Updated check and fix to include log-input on deny statement.

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

CISC-ND-000140

CISC-ND-000140 - Updated check and fix to include log-input on deny statement.

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

CISC-RT-000020

CISC-RT-000020 - Updated vulnerability discussion to provide clarification of the requirement.

CISC-RT-000080

CISC-RT-000080 - Updated check to provide clarification of the requirement.

CISC-RT-000235

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

CISC-RT-000236

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

CISC-RT-000237

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

CISC-RT-000391

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

CISC-RT-000392

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

CISC-RT-000393

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

CISC-RT-000394

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

CISC-RT-000395

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

CISC-RT-000396

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

CISC-RT-000397

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

CISC-RT-000398

CISC-RT-000398 - Added requirement to drop IPv6 packets containing a Hop-by-Hop or Destination Option extension header with an undefined option type.

EDB Postgres Advanced Server STIG, Version 2, Release 1

PPS9-00-009500

PPS9-00-009500 - Changed how to configure SSL.

PPS9-00-009600

PPS9-00-009600 - Changed how to configure SSL.

EDB Postgres Advanced Server v11 on Windows STIG, Version 2, Release 1

EP11-00-001200

EP11-00-001200 - Combined audit requirements.

EP11-00-001300

EP11-00-001300 - Combined with EP11-00-001200.

EP11-00-001600

EP11-00-001600 - Combined with EP11-00-001200.

EP11-00-001700

EP11-00-001700 - Combined with EP11-00-001200.

EP11-00-001800

EP11-00-001800 - Combined with EP11-00-001200.

EP11-00-001900

EP11-00-001900 - Combined with EP11-00-001200.

EP11-00-002000

EP11-00-002000 - Combined with EP11-00-001200.

EP11-00-002100

EP11-00-002100 - Combined with EP11-00-001200.

EP11-00-008600

EP11-00-008600 - Combined with EP11-00-001200.

EP11-00-009500

EP11-00-009500 - Changed how to configure SSL.

EP11-00-009600

EP11-00-009600 - Changed how to configure SSL.

EP11-00-010000

EP11-00-010000 - Combined with EP11-00-001200.

EP11-00-010100

EP11-00-010100 - Combined with EP11-00-001200.

EP11-00-010200

EP11-00-010200 - Combined with EP11-00-001200.

EP11-00-010300

EP11-00-010300 - Combined with EP11-00-001200.

EP11-00-010400

EP11-00-010400 - Combined with EP11-00-001200.

EP11-00-010500

EP11-00-010500 - Combined with EP11-00-001200.

EP11-00-010600
EP11-00-010600 - Combined with EP11-00-001200.

EP11-00-010700
EP11-00-010700 - Combined with EP11-00-001200.

EP11-00-010800
EP11-00-010800 - Combined with EP11-00-001200.

EP11-00-010900
EP11-00-010900 - Combined with EP11-00-001200.

EP11-00-011000
EP11-00-011000 - Combined with EP11-00-001200.

EP11-00-011050
EP11-00-011050 - Combined with EP11-00-001200.

EP11-00-011100
EP11-00-011100 - Combined with EP11-00-001200.

EP11-00-011150
EP11-00-011150 - Combined with EP11-00-001200.

EP11-00-011200
EP11-00-011200 - Combined with EP11-00-001200.

EP11-00-011300
EP11-00-011300 - Combined with EP11-00-001200.

EP11-00-011400
EP11-00-011400 - Combined with EP11-00-001200.

EP11-00-011500
EP11-00-011500 - Combined with EP11-00-001200.

EP11-00-011600
EP11-00-011600 - Combined with EP11-00-001200.

EP11-00-011700
EP11-00-011700 - Combined with EP11-00-001200.

EP11-00-012000
EP11-00-012000 - Combined with EP11-00-001200.

EP11-00-012100
EP11-00-012100 - Combined with EP11-00-001200.

EP11-00-012400
EP11-00-012400 - Combined with EP11-00-001200.

EP11-00-012500
EP11-00-012500 - Combined with EP11-00-001200.

F5 BIG-IP Access Policy Manager 11.x STIG, Version 2, Release 1

F5BI-AP-000147
F5BI-AP-000147 - Changed Parent SRG to SRG-NET-000517-ALG-000006, CCI-002361.

F5BI-AP-000151
F5BI-AP-000151 - Changed the Parent SRG to SRG-NET-000519-ALG-000008, CCI-002364.

F5BI-AP-000197
F5BI-AP-000197 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60033, CCI-000766.

F5BI-AP-000199
F5BI-AP-000199 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60033, CCI-000766.

F5BI-AP-000205

F5BI-AP-000205 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60033, CCI-000766.

F5BI-AP-000207

F5BI-AP-000207 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60033, CCI-000766.

F5BI-AP-000209

F5BI-AP-000209 - Removed requirement; it is no longer in the parent SRG. Check and fix are redundant to V-60061.

F5 BIG-IP Device Management 11.x STIG, Version 2, Release 1

F5BI-DM-000290

F5BI-DM-000290 - Added a policy to APM stating if F5 is being used to authenticate users for web applications, the HTTP_Only flag must be set.

F5 BIG-IP Local Traffic Manager 11.x STIG, Version 2, Release 1

F5BI-LT-000139

F5BI-LT-000139 - Changed Parent SRG to SRG-NET-000521-ALG-000002, CCI-001494.

F5BI-LT-000141

F5BI-LT-000141 - Changed Parent SRG to SRG-NET-000514-ALG-000514, CCI-000057.

F5BI-LT-000143

F5BI-LT-000143 - Changed Parent SRG to SRG-NET-000515-ALG-000515, CCI-000058.

F5BI-LT-000147

F5BI-LT-000147 - Changed Parent SRG to SRG-NET-000517-ALG-000006, CCI-002361.

F5BI-LT-000151

F5BI-LT-000151 - Changed Parent SRG to SRG-NET-000519-ALG-000008, CCI-002364.

F5BI-LT-000197

F5BI-LT-000197 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60303, CCI-000766.

F5BI-LT-000199

F5BI-LT-000199 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60303, CCI-000766.

F5BI-LT-000205

F5BI-LT-000205 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60303, CCI-000766.

F5BI-LT-000207

F5BI-LT-000207 - Removed requirement; it is no longer in the parent SRG. It is covered by V-60303, CCI-000766.

F5BI-LT-000209

F5BI-LT-000209 - Removed requirement; it is no longer in the parent SRG. Check and fix are redundant to V-60357.

Google Chrome for Windows STIG Benchmark, Version 2, Release 1

DTBC-0004

Rebundled to capture the change in the text for SV-57553.

NA

Repackaged benchmark to include updated STIG IDs.

Google Chrome STIG, Version 2, Release 1

DTBC-0004

DTBC-0004 - Added whitelisting clause.

DTBC-0008

DTBC-0008 - Corrected URL syntax.

HBSS Agent Handler STIG , Version 2, Release 1

NA

Modified Overview to state that the Agent Handler STIG does not need to be applied if the only Agent Handler is the ePO server itself.

HBSS ePO 5.x STIG, Version 2, Release 1

H30243

H30243 - Corrected the McAfee Agent communication port.

H30700

H30700 - Modified the check criteria for a File Integrity Monitor.

H31165

H31165 - Modified check criteria to match requirement.

H42130

H42130 - Modified verbiage regarding USCYBERCOM order to read OPORD instead of TASKORD.

H60100

H60100 - Modified verbiage for clarity in meeting the requirement of log file retentions.

H60120

H60120 - Modified verbiage for clarity when defining log files to be audited.

HBSS HIP 8 STIG, Version 5, Release 1

H36664

H36664 - Added exception for servers with application with a web interface for administration.

HBSS McAfee Agent, Version 5, Release 1

H36120

H36120 - Modified requirement to reflect the transition of using ACCM to Policy Auditor.

IBM AIX 7.x STIG, Version 2, Release 1

AIX7-00-001025

AIX7-00-001025 - Updated an incorrect file path in the check content.

AIX7-00-002070

AIX7-00-002070 - Updated the requirement to allow for file ownership by a system account.

AIX7-00-002071

AIX7-00-002071 - Updated the requirement to allow for file group ownership by a system group.

AIX7-00-003143

AIX7-00-003143 - Updated the parent SRG ID assigned to this requirement.

ISEC7 Sphere STIG, Version 2, Release 1

ISEC-OO-000100

ISEC-OO-000100 - Added new requirement stating server version must be a vendor-supported version.

NA

Updated STIG file name, Overview, and Supplemental document titles and text to reflect new brand name of ISEC7 server. ISEC7 EMM Suite is now ISEC7 Sphere.

Juniper SRX SG ALG STIG, Version 2, Release 1

JUSX-AG-000120

JUSX-AG-000120 - Changed "sin" to "syn" in fix text.

McAfee Application Control 8.x STIG, Version 2, Release 1

MCAC-TE-000115

MCAC-TE-000115 - Provided clarification for inventory interval option for Virtual Desktop Infrastructure (VDI) master images.

McAfee ENS 10.x STIG, Version 2, Release 1

ENS-CO-000106

ENS-CO-000106 - Modified check criteria to state size to be between 50-100 MB.

ENS-CO-000108

ENS-CO-000108 - Modified check criteria to allow for syslog as a logging destination.

ENS-CO-000111

ENS-CO-000111 - Added requirement for Proxy server configuration setting.

ENS-CO-000112

ENS-CO-000112 - Added requirement for Default Client Update settings.

ENS-CO-000114

ENS-CO-000114 - Added requirement for ENS Managed Tasks.

ENS-CO-000115

ENS-CO-000115 - Added requirement for validating latest in DISA Patch Repository for mandated version.

ENS-EP-000001

ENS-EP-000001 - Added requirement for enabling IPS.

ENS-EP-000002

ENS-EP-000002 - Added requirement for Generic Privilege Escalation Prevention.

ENS-EP-000003

ENS-EP-000003 - Added requirement for Windows Data Execution Prevention.

ENS-EP-000004

ENS-EP-000004 - Added requirement for ENS McAfee Custom Content.

ENS-FW-000001

ENS-FW-000001 - Added requirement for enabling firewall intrusion alerts.

ENS-FW-000002

ENS-FW-000002 - Added requirement for Firewall Status Control setting.

ENS-FW-000003

ENS-FW-000003 - Added requirement for enabling firewall (disabling adaptive mode and disabling client side rules).

ENS-FW-000005

ENS-FW-000005 - Added requirement for allowing all outbound TCP traffic.

ENS-FW-000006

ENS-FW-000006 - Added requirement for disabling IP protocol 41.

ENS-FW-000007

ENS-FW-000007 - Added requirement for logging all blocked firewall traffic.

ENS-FW-000008

ENS-FW-000008 - Added requirement for McAfee GTI Network Reputation.

ENS-FW-000009

ENS-FW-000009 - Added requirement for stateful firewall.

ENS-FW-000010

ENS-FW-000010 - Added requirement for FTP protocol inspection.

ENS-TP-000237

ENS-TP-000237 - Modified requirement for system utilization to be set to "Limit to Maximum CPU Usage".

ENS-TP-000238

ENS-TP-000238 - Added N/A note for Linux systems.

ENS-TP-000243

ENS-TP-000243 - Added N/A note for Linux systems.

ENS-TP-000245

ENS-TP-000245 - Added requirement for enabling McAfee GTI in On-Demand Scan.

McAfee TIE/DXL STIG, Version 2, Release 1

TIDX-CL-000007

TIDX-CL-000007 - Removed requirement for requiring client to connect to the TIE server.

TIDX-SV-000001

TIDX-SV-000001 - Modified check criteria to remove criteria for review OS version.

TIDX-SV-000002

TIDX-SV-000002 - Removed requirement for proxy settings.

TIDX-SV-000004

TIDX-SV-000004 - Modified requirement for disabling GTI on Classified networks.

TIDX-SV-000013

TIDX-SV-000013 - Removed not applicable requirement.

TIDX-SV-000014

TIDX-SV-000014 - Removed requirement for web gateway integration.

TIDX-SV-000015

TIDX-SV-000015 - Removed requirement for configuring log level to WARN.

TIDX-VS-000001

TIDX-VS-000001 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000002

TIDX-VS-000002 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000003

TIDX-VS-000003 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000004

TIDX-VS-000004 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000005

TIDX-VS-000005 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000006

TIDX-VS-000006 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000007

TIDX-VS-000007 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000008

TIDX-VS-000008 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000009

TIDX-VS-000009 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000010

TIDX-VS-000010 - Removed requirement for TIE module for VSE settings.

TIDX-VS-000011

TIDX-VS-000011 - Removed requirement for TIE module for VSE settings.

Microsoft Exchange 2016 Edge Transport Server STIG, Version 2, Release 1

EX16-ED-000300

EX16-ED-000300 - Modified verbiage to add IMAP Secure as viable option.

EX16-ED-003020

EX16-ED-003020 - Removed the requirement for DoD-approved Exchange-aware code protection.

Microsoft Exchange 2016 Mailbox Server STIG, Version 2, Release 1

EX16-MB-000180

EX16-MB-000180 - Modified verbiage to add IMAP Secure as viable option.

EX16-MB-000220

EX16-MB-000220 - Clarified options for check criteria.

EX16-MB-000360

EX16-MB-000360 - Modified verbiage to add IMAP Secure as viable option.

EX16-MB-000600

EX16-MB-000600 - Modified verbiage to add IMAP Secure as viable option.

EX16-MB-002890

EX16-MB-002890 - Removed the requirement for DoD-approved Exchange-aware code protection.

Microsoft IIS 10.0 Server STIG, Version 2, Release 1

IIST-SV-000115

IIST-SV-000115 - Modified check and fix.

IIST-SV-000132

IIST-SV-000132 - Added N/A Clause for Exchange.

Microsoft IIS 10.0 Site STIG, Version 2, Release 1

IIST-SI-000242

IIST-SI-000242 - Added N/A for WSUS clause.

Microsoft IIS 8.5 Server STIG, Version 2, Release 1

IISW-SV-000151

IISW-SV-000151 - Modified check and fix.

IISW-SV-000157

IISW-SV-000157 - Removed requirement.

IISW-SV-000159

IISW-SV-000159 - Added N/A statement for WSUS clause.

Microsoft IIS 8.5 Site STIG, Version 2, Release 1

IISW-SI-000203

IISW-SI-000203 - Added N/A for WSUS clause.

IISW-SI-000204

IISW-SI-000204 - Added N/A for WSUS clause.

IISW-SI-000246

IISW-SI-000246 - Modified check and fix.

Microsoft Office 365 ProPlus STIG, Version 2, Release 1

O365-CO-000001

O365-CO-000001 - Corrected registry key value for validation.

O365-CO-000003

O365-CO-000003 - Added CCI and NIST controls from removed STIG ID O365-CO-000011 as both requirements were the same.

O365-CO-000011

O365-CO-000011 - Removed the requirement. Duplicate of V-99649. Added CCI control to V99649.

O365-EX-000030

O365-EX-000030 - Corrected Registry key required value.

Microsoft Office System 2013 STIG, Version 2, Release 1

DTOO193

DTOO193 - Correct registry key to remove directions about "for every user profile hive".

DTOO199

DTOO199 - Corrected registry key to remove directions about "for every user profile hive".

Microsoft Outlook 2016 STIG, Version 2, Release 1

DT00262

DT00262 - Modified Vulnerability Discussion to provided information regarding encryption in FIPS mode.

Microsoft SQL Server 2016 Database STIG, Version 2, Release 1

SQL6-D0-000300

SQL6-D0-000300 - Updated supplemental script.

Microsoft SQL Server 2016 Instance STIG, Version 2, Release 1

SQL6-D0-005900

SQL6-D0-005900 - Added N/A statement - application or security event log use.

SQL6-D0-006000

SQL6-D0-006000 - Combined requirement with SQL6-D0-005900.

SQL6-D0-006100

SQL6-D0-006100 - Combined requirement with SQL6-D0-005900.

Microsoft Windows 2012 Server Domain Name System STIG, Version 2, Release 1

WDNS-AC-000001

WDNS-AC-000001 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-AU-000001

WDNS-AU-000001 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-AU-000005

WDNS-AU-000005 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-AU-000006

WDNS-AU-000006 - Combined V-58555, V-58563, V-58561, V-58565, V-58567, V-58569, V-58571 and V-58719 into this requirement and combined CCI controls.

WDNS-AU-000008

WDNS-AU-000008 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-AU-000010

WDNS-AU-000010 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-AU-000011

WDNS-AU-000011 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-AU-000012

WDNS-AU-000012 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-AU-000013

WDNS-AU-000013 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-AU-000014

WDNS-AU-000014 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-AU-000015

WDNS-AU-000015 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-CM-000001

WDNS-CM-000001 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000003

WDNS-CM-000003 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000004

WDNS-CM-000004 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000006

WDNS-CM-000006 - Modified Fix Text to specify to implement mechanisms to assure caching server validates signed zones.

WDNS-CM-000009

WDNS-CM-000009 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000010

WDNS-CM-000010 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000013

WDNS-CM-000013 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000014

WDNS-CM-000014 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000015

WDNS-CM-000015 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000016

WDNS-CM-000016 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000019

WDNS-CM-000019 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000020

WDNS-CM-000020 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000021

WDNS-CM-000021 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000024

WDNS-CM-000024 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000025

WDNS-CM-000025 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000026

WDNS-CM-000026 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000027

WDNS-CM-000027 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000028

WDNS-CM-000028 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-CM-000028 - Added clarification on when IPv6 configuration.

WDNS-IA-000001

WDNS-IA-000001 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-IA-000002

WDNS-IA-000002 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-IA-000004

WDNS-IA-000004 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-IA-000009

WDNS-IA-000009 - Added clarification regarding applicability if a caching server.

WDNS-SC-000001

WDNS-SC-000001 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000003

WDNS-SC-000003 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000006

WDNS-SC-000006 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000009

WDNS-SC-000009 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000010

WDNS-SC-000010 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.
WDNS-SC-000010 - Corrected Fix text to specify configuring a caching server to validate signed zones.

WDNS-SC-000013

WDNS-SC-000013 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000014

WDNS-SC-000014 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000019

WDNS-SC-000019 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000022

WDNS-SC-000022 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.
WDNS-SC-000022 - Added caveat that if caching server requirement is N/A.

WDNS-SC-000025

WDNS-SC-000025 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SC-000027

WDNS-SC-000027 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SI-000001

WDNS-SI-000001 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

WDNS-SI-000009

WDNS-SI-000009 - Same check and fix as V-58551. Combined into V-59551 and combined CCI controls.

WDNS-SC-000031

WDNS-SC-000031 - Modified check and fix verbiage to add Local Administrator as logon account for DNS servers not part of the domain.

Oracle Linux 6 STIG, Version 2, Release 1

OL6-00-000061

OL6-00-000061 - Updated fix text to set unlock_time to 900.

OL6-00-000356

OL6-00-000356 - Updated check and fix text on unlock_time.

OL6-00-000357

OL6-00-000357 - Updated fix text to set unlock_time to 900.

OL6-00-000529

OL6-00-000529 - Updated check content and finding statement to require documented authorized use of "NOPASSWD" or "!authenticate"

Oracle Linux 7 STIG , Version 2, Release 1

OL07-00-010010

OL07-00-010010 - Updated check and fix text; also updated CCIs.

OL07-00-010020

OL07-00-010020 - Updated check text and CCIs.

OL07-00-010040

OL07-00-010040 - Removed specific references to GNOME and replaced with Graphical User Interface.

OL07-00-010090

OL07-00-010090 - Removed requirement.

OL07-00-010100

OL07-00-010100 - Added not applicable statement to the check text.

OL07-00-010219

OL07-00-010219 - Removed the requirement.

OL07-00-010320

OL07-00-010320 - Updated rule title, check text, and CCIs.

OL07-00-010340

OL07-00-010340 - Updated check content and finding statement to require documented authorized use of "NOPASSWD" or "!authenticate"

OL07-00-010350

OL07-00-010350 - Added requirement for users to re-authenticate for privilege escalation.

OL07-00-020020

OL07-00-020020 - Updated check, fix, and CCIs.

OL07-00-020030

OL07-00-020030 - Updated check text example output.

OL07-00-020040

OL07-00-020040 - Updated check text example output and upgraded severity to a CAT II.

OL07-00-020100

OL07-00-020100 - Updated check, fix, and CCIs.

OL07-00-020101

OL07-00-020101 - Updated check text to include verification that the DCCP kernel module is disabled.

OL07-00-020111

OL07-00-020111 - Added new requirement to check the graphical user interface automoutner is disabled.

OL07-00-020210

OL07-00-020210 - Downgraded to a CAT II and added verbiage to the check text.

OL07-00-020220

OL07-00-020220 - Added requirement for SELinux targeted policy.

OL07-00-020230

OL07-00-020230 - Removed references to GNOME.

OL07-00-020231

OL07-00-020231- Added requirement to disable Ctrl-Alt-Delete key sequence for the Graphical User Interface.

OL07-00-020600

OL07-00-020600 - Removed requirement.

OL07-00-020620

OL07-00-020620 - Updated rule title, vulnerability discussion, and check text.

OL07-00-020690

OL07-00-020690 - Updated check and fix text.

OL07-00-020700

OL07-00-020700 - Updated commands in check and fix text.

OL07-00-020710

OL07-00-020710 - Updated commands in check and fix text.

OL07-00-021022

OL07-00-021022 - Combined requirement with OL07-00-021024.

OL07-00-021023

OL07-00-021023 - Combined requirement with OL07-00-021024.

OL07-00-021024

OL07-00-021024 - Updated requirement to combine OL07-00-021022 and OL07-00-021023.

OL07-00-021030

OL07-00-021030 - Updated vulnerability discussion, check, and fix text to elaborate on possible group owners.

OL07-00-021031

OL07-00-021031 - Added new requirement to check that world-writable directories are owned by root, sys, bin, or an application account.

OL07-00-021340

OL07-00-021340 - Fixed typo in check text finding statement from "and" to "or".

OL07-00-021350

OL07-00-021350 - Updated check and fix text to verify existence of a key file for FIPS compliance.

OL07-00-021620

OL07-00-021620 - Updated vulnerability discussion and check text.

OL07-00-030000

OL07-00-030000 - Downgraded to a CAT II.

OL07-00-030010

OL07-00-030010 - Updated check text and CCIs.

OL07-00-030200

OL07-00-030200 - Removed requirement.

OL07-00-030201

OL07-00-030201 - Updated rule title, vulnerability discussion, and check text to allow for alternative methods of off-loading audit logs.

OL07-00-030210

OL07-00-030210 - Updated check text to allow for additional methods of audit log off-load.

OL07-00-030211

OL07-00-030211 - Updated check text to allow for additional methods of audit log off-load.

OL07-00-030320

OL07-00-030320 - Updated check text to allow for additional methods of audit log off-load.

OL07-00-030321

OL07-00-030321 - Updated check text to allow for additional methods of audit log off-load.

OL07-00-030330

OL07-00-030330 - Fixed typo in check and fix text.

OL07-00-030360

OL07-00-030360 - Updated vulnerability discussion, check, and fix text.

OL07-00-030370

OL07-00-030370 - Updated vulnerability discussion, check text, fix text, and CCIs.

OL07-00-030380

OL07-00-030380 - Updated vulnerability discussion, check text, fix text, and CCIs.

OL07-00-030390

OL07-00-030390 - Updated vulnerability discussion, check text, fix text, and CCIs.

OL07-00-030400

OL07-00-030400 - Updated vulnerability discussion, check text, fix text, and CCIs.

OL07-00-030410

OL07-00-030410 - Updated vulnerability discussion, check, and fix text.

OL07-00-030420

OL07-00-030420 - Updated vulnerability discussion, check, and fix text.

OL07-00-030430

OL07-00-030430 - Updated vulnerability discussion, check, and fix text.

OL07-00-030440

OL07-00-030440 - Updated vulnerability discussion, check, and fix text.

OL07-00-030450

OL07-00-030450 - Updated vulnerability discussion, check, and fix text.

OL07-00-030460

OL07-00-030460 - Updated vulnerability discussion, check, and fix text.

OL07-00-030470

OL07-00-030470 - Updated vulnerability discussion, check, and fix text.

OL07-00-030480

OL07-00-030480 - Updated vulnerability discussion, check, and fix text.

OL07-00-030490

OL07-00-030490 - Updated vulnerability discussion, check, and fix text.

OL07-00-030500

OL07-00-030500 - Updated vulnerability discussion, check, and fix text.

OL07-00-030510

OL07-00-030510 - Updated vulnerability discussion, check, and fix text.

OL07-00-030520

OL07-00-030520 - Updated vulnerability discussion, check, and fix text.

OL07-00-030530

OL07-00-030530 - Updated vulnerability discussion, check, and fix text.

OL07-00-030540

OL07-00-030540 - Updated vulnerability discussion, check, and fix text.

OL07-00-030550

OL07-00-030550 - Updated vulnerability discussion, check, and fix text.

OL07-00-030740

OL07-00-030740 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030819

OL07-00-030819 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030821

OL07-00-030821 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030880

OL07-00-030880 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030890

OL07-00-030890 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030900

OL07-00-030900 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030910

OL07-00-030910 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-030920

OL07-00-030920 - Updated check and fix text to include both 32-bit and 64-bit architectures.

OL07-00-040000

OL07-00-040000 - Updated check and fix text to include additional directory for setting maxlogins.

OL07-00-040170

OL07-00-040170 - Updated check and fix text verbiage.

OL07-00-040180

OL07-00-040180 - Updated check text with a not applicable statement.

OL07-00-040190

OL07-00-040190 - Updated check text with a not applicable statement.

OL07-00-040200

OL07-00-040200 - Updated check text with a not applicable statement.

OL07-00-040500

OL07-00-040500 - Updated check and fix text to include additional ntp service.

OL07-00-040600

OL07-00-040600 - Updated rule title and check text.

OL07-00-040730

OL07-00-040730 - Generalized overall requirement to cover any graphical display managers.

OL07-00-041001

OL07-00-041001 - Updated vulnerability discussion, check, fix, and CCIs.

Oracle Linux 7 STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

OL07-00-010090

OL07-00-010090 - Remove the rule from the benchmark because the rule is being removed from the STIG.

OL07-00-020030

Updated OVAL to not require "root" in the "/var/spool/cron/root" entry for "aide".

OL07-00-020600

OL07-00-020600 - Remove the rule from the benchmark because the rule is being removed from the STIG.

OL07-00-021030

Updated OVAL to check GID, rather than UID.

OL07-00-021350

Updated OVAL to verify FIPS status more consistently.

OL07-00-030000

OL07-00-030000 - Rebundle to capture the change of SV-108371 to a CAT 2.

OL07-00-030200

OL07-00-030200 - Remove the rule from the benchmark because the rule is being removed from the STIG.

OL07-00-030740

Updated OVAL to accept the "-F perm=x" option and variations thereof.

OL07-00-040110

Updated OVAL to verify FIPS status more consistently.

OL07-00-040400

Updated OVAL to verify FIPS status more consistently.

OL07-00-041001

OL07-00-041001 - Update the OVAL to match the change in check text.

Palo Alto Networks ALG STIG , Version 2, Release 1

PANW-AG-000062

PANW-AG-000062 - Changed check and fix action. Changed "Action" setting value to "drop" or “reset-both”.

PANW-AG-000063

PANW-AG-000063 - Changed check and fix action. Changed "Action" setting value to "drop" or “reset-both”.

PANW-AG-000073

PANW-AG-000073 - Changed check and fix action. Changed "Action" setting value to "drop" or “reset-both”.

PANW-AG-000074

PANW-AG-000074 - Changed check and fix action. Changed "Action" setting value to "drop" or “reset-both”.

Palo Alto Networks IDPS STIG, Version 2, Release 1

PANW-IP-000008

PANW-IP-000008 - Changed to CAT III. Added note to fix text that this will only capture the first packet.

PostgresSQL 9.x STIG, Version 2, Release 1

PGS9-00-002500

PGS9-00-002500 - Updated client_min_messages setting.

PGS9-00-003000

PGS9-00-003000 - Changed how to configure SSL.

PGS9-00-007200

PGS9-00-007200 - Changed how to configure SSL.

Red Hat Enterprise Linux 6 STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

RHEL-06-000356

RHEL-06-000356 - Update the OVAL to match the change in check text.

Red Hat Enterprise Linux 6 STIG, Version 2, Release 1

RHEL-06-000061

RHEL-06-000061 - Updated fix text to set unlock_time to 900.

RHEL-06-000356

RHEL-06-000356 - Updated check and fix text on unlock_time.

RHEL-06-000357

RHEL-06-000357 - Updated fix text to set unlock_time to 900.

RHEL-06-000529

RHEL-06-000529 - Updated check content and finding statement to require documented authorized use of "NOPASSWD" or "!authenticate"

Red Hat Enterprise Linux 7 STIG Benchmark, Version 3, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

RHEL-07-020030

Updated OVAL to not require "root" in the "/var/spool/cron/root" entry for "aide".

RHEL-07-021030

Updated OVAL to check GID, rather than UID.

RHEL-07-030000

Rebundle to capture the change of SV-86703 to a CAT 2.

RHEL-07-030740

Updated OVAL to accept the "-F perm=x" option and variations thereof.

Red Hat Enterprise Linux 7 STIG, Version 3, Release 1

RHEL-07-010010

RHEL-07-010010 - Fixed typos in the check text command.

RHEL-07-010340

RHEL-07-010340 - Updated check content and finding statement to require documented authorized use of "NOPASSWD" or "!authenticate".

RHEL-07-020030

RHEL-07-020030 - Updated check text example output.

RHEL-07-020040

RHEL-07-020040 - Updated check text example output.

RHEL-07-020111

RHEL-07-020111 - Added not applicable statement to the check text.

RHEL-07-020210

RHEL-07-020210 - Downgraded to a CAT II.

RHEL-07-020220

RHEL-07-020220 - Downgraded to a CAT II.

RHEL-07-021030

RHEL-07-021030 - Updated vulnerability discussion, check, and fix to elaborate possible group owners.

RHEL-07-021031

RHEL-07-021031 - Added requirement to check that world-writable directories are owned by root, sys, bin, or an application account.

RHEL-07-021340

RHEL-07-021340 - Fixed typo in check text finding statement from "and" to "or".

RHEL-07-021350

RHEL-07-021350 - Updated check and fix text to verify existence of a key file for FIPS compliance.

RHEL-07-030000

RHEL-07-030000 - Downgraded to a CAT II.

RHEL-07-030210

RHEL-07-030210 - Updated check text to allow for additional methods of audit log off-load.

RHEL-07-030211

RHEL-07-030211 - Updated check text to allow for additional methods of audit log off-load.

RHEL-07-030320

RHEL-07-030320 - Updated check text to allow for additional methods of audit log off-load.

RHEL-07-030321

RHEL-07-030321 - Updated check text to allow for additional methods of audit log off-load.

RHEL-07-040730

RHEL-07-040730 - Generalized overall requirement to cover any graphical display managers.

RHEL-07-910055

RHEL-07-910055 - Added requirement to protect audit information.

Solaris 10 SPARC STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

Solaris 10 SPARC STIG, Version 2, Release 1

GEN003503

GEN003503 - Updated fix text to elaborate possible group owners.

Solaris 10 X86 STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

Solaris 10 x86 STIG, Version 2, Release 1

GEN003503

GEN003503 - Updated fix text to elaborate possible group owners.

Solaris 11 SPARC STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

Solaris 11 SPARC STIG, Version 2, Release 1

SOL-11.1-010440

SOL-11.1-010440 - Combined SOL-11.1-01045 and SOL-11.1-010460 into this requirement.

SOL-11.1-010450

SOL-11.1-010450 - Combined requirement with SOL-11.1-010440.

SOL-11.1-010460

SOL-11.1-010460 - Combined requirement with SOL-11.1-010440.

SOL-11.1-040280

SOL-11.1-040280 - Updated vulnerability discussion and added CCI-000795.

SOL-11.1-040290

SOL-11.1-040290 - Removed requirement.

SOL-11.1-040300

SOL-11.1-040300 - Removed requirement.

SOL-11.1-080060

SOL-11.1-080060 - Updated rule title, check, and fix text to elaborate possible group owners.

SOL-11.1-090280

SOL-11.1-090280 - Updated check and fix text to include specific commands based on OS version.

Solaris 11 X86 STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

Solaris 11 x86 STIG, Version 2, Release 1

SOL-11.1-010440

SOL-11.1-010440 - Combined with SOL-11.1-010450 and SOL-11.1-010460.

SOL-11.1-010450

SOL-11.1-010450 - Combined requirement with SOL-11.1-010440.

SOL-11.1-010460

SOL-11.1-010460 - Combined requirement with SOL-11.1-010440.

SOL-11.1-040280

SOL-11.1-040280 - Updated vulnerability discussion and added CCI-000795.

SOL-11.1-040290

SOL-11.1-040290 - Removed requirement.

SOL-11.1-040300

SOL-11.1-040300 - Removed requirement.

SOL-11.1-080060

SOL-11.1-080060 - Updated rule title, check, and fix text to elaborate possible group owners.

SOL-11.1-090280

SOL-11.1-090280 - Updated check and fix text to include specific commands based on OS version.

Splunk Enterprise 7.x for Windows STIG, Version 2, Release 1

SPLK-CL-000270

SPLK-CL-000270 - Updated Rule Title, Check, and Fix to address the CCI control.

SUSE Linux Enterprise Server 12 STIG Benchmark, Version 2, Release 1

NA

Repackaged benchmark to include updated STIG IDs.

SUSE Linux Enterprise Server 12 STIG, Version 2, Release 1

SLES-12-010040

SLES-12-010040 - Updated fix text to include command to update the system database as part of the fix.

SLES-12-010070

SLES-12-010070 - Removed incorrect statement referencing a graphical user interface in the check text.

SLES-12-010130

SLES-12-010130 - Updated rule title, vulnerability discussion, check, fix, and CCIs.

SLES-12-010131

SLES-12-010131 - Combined requirement with SLES-12-010130.

Virtual Private Network (VPN) SRG, Version 2, Release 1

SRG-NET-000341-VPN-001350

SRG-NET-000341-VPN-001350 - Clarified this requirement is for user connectivity using the VPN function of the product, and uses CAC/PKI instead of PIV.

SRG-NET-000342-VPN-001360

SRG-NET-000342-VPN-001360 - Clarified this requirement is for user connectivity using the VPN function of the product, and uses CAC/PKI instead of PIV.

Voice Video Session Management SRG, Version 1, Release 7

SRG-NET-000338-VVSM-00056

SRG-NET-000338-VVSM-00056 - Updated the requirement for better clarity of explanation

z/OS SRR Scripts, Version 6, Release 47

ACF2-OS-000100

ACF2-OS-000100 - Corrected processing SMFPRMxx member that have sequence numbers.

NA

Corrected the processing of the CICS product for TSS.
Made changes to initialize variable within script.

RACF-ES-000160

RACF-ES-000160 - Made changes on processing PROGRAM profiles that contain masking.

RACF-OS-000130

RACF-OS-000130 - Corrected processing SMFPRMxx member that have sequence numbers.

TSS0-OS-000050

TSS0-OS-000050 - Corrected processing SMFPRMxx member that have sequence numbers.

ZADT0002

ZADT0002 - Made changes to evaluation to allow READ access to all users.

ZTAD0000

ZTAD0000 - Made changes to evaluation to allow READ access to all users.

zOS ACF2 STIG , Version 8, Release 1

ACF2-ES-000410

ACF2-ES-000410 - Deleted requirement; duplicate of ACF2-US-000040.

ACF2-US-000040

ACF2-US-000040 - Allowed authorized users to BPX.SRV profiles.

zOS ACF2 STIG, Version 8, Release 1

ACF2-UT-000030

ACF2-UT-000030 - Reworded title to add check for otelnet banner.

zOS RACF STIG, Version 8, Release 1

ACF2-ES-000140

ACF2-ES-000140 - Reworded check to address addition of SSP authorized users.

ACF2-ES-000220

ACF2-ES-000220 - Reworded check to address addition of SSP authorized users.

RACF-ES-000160

RACF-ES-000160 - Removed logging requirement.

RACF-ES-000180

RACF-ES-000180 - Reworded check to address addition of SSP authorized users.

RACF-ES-000210

RACF-ES-000210 - Reworded check to address addition of SSP authorized users.

RACF-ES-000490

RACF-ES-000490 - Revised rule title.

RACF-ES-000510

RACF-ES-000510 - Deleted requirement.

RACF-ES-000660

RACF-ES-000660 - Corrected Title, check and Fix

RACF-ES-000670

RACF-ES-000670 - Deleted requirement.
RACF-ES-000670 - Corrected Title, check and Fix

RACF-ES-000720

RACF-ES-000720 - Combined requirement with RACF-ES-000730.

RACF-ES-000810

RACF-ES-000810 - Delete requirement.

RACF-FT-000040

RACF-FT-000040 - Reworded title to indicate that the content must be checked.

RACF-FT-000060

RACF-FT-000060 - Deleted requirement; duplicate of RACF-FT-0000040.

RACF-OS-000230

RACF-OS-000230 - Deleted requirement; duplicate of RACF-OS-000100.

RACF-OS-000320

RACF-OS-000320 - Corrected typo DS880 should be DS8880.

RACF-OS-000330

RACF-OS-000330 - Corrected typo DS880 should be DS8880.

RACF-OS-000340

RACF-OS-000340 - Corrected typo DS880 should be DS8880.

RACF-SH-000060

RACF-SH-000060 - Deleted requirement.

RACF-TC-000050

RACF-TC-000050 - Deleted requirement.

RACF-TC-000090

RACF-TC-000090 - Deleted requirement.

RACF-TN-000040

RACF-TN-000040 - Reworded title to indicate that the content must be checked.

RACF-TN-000060

RACF-TN-000060 - Deleted requirement; duplicate of RACF-TN-0000010.

RACF-US-000010

RACF-US-000010 - Corrected resource to resources in the title.

RACF-ES-000365

RACF-ES-000365 - Added requirement for Password Phrase controls for RACF.

RACF-US-000070

RACF-US-000070 - Reworded to allow authorized users to BPX.SRV profiles.

RACF-US-000130

RACF-US-000130 - Deleted requirement.

RACF-US-000260

RACF-US-000260 - Removed BPX.DEFAULT.USER from the FIX example.

RACF-UT-000030

RACF-UT-000030 - Reworded title to add check for otelnet banner.

TSS0-ES-000310

TSS0-ES-000310 - Reworded check to address addition of SSP authorized users.

TSS0-ES-000320

TSS0-ES-000320 - Reworded check to address addition of SSP authorized users.

zOS TSS STIG, Version 8, Release 1

TSS0-US-000040

TSS0-US-000040 - Reworded to allow authorized users to BPX.SRV profiles.

TSS0-UT-000010

TSS0-UT-000010 - Reworded title to add check for otelnet banner.