# JULY 2017 MAINTENANCE RELEASE: STIGS TO BE RELEASED

## Adobe ColdFusion 11 STIG, Version 1, Release 3

**V-62491**

V-62491 Update check. Change "Maximum number of simultaneous CFC function requests" to "Maximum number of simultaneous Web Service requests".

**V-62493**

V-62493 Update check. Check content has a typo in the fourth paragraph of the Check Content: If the CFC requests are not being used b hosted applications and "Maximum number of simultaneous CFC function requests" is not set to 1, this is a finding.

## Apache Site 2.2 for Windows STIG, Version 1, Release 11

**Documentation Update**

Repackaged STIG due to STIG name discrepancy in last release.

## Apple OS X 10.11 STIG, Version 1, Release 5

**V-67741**

Updated V-67741 Check and Fix instructions to reflect specific Internet sharing settings.

**Documentation Update**

Updated Custom Policy configuration profile for Internet sharing settings.

Updated Overview document to accurately reflect FIPS 140-2 validated cryptographic modules.

## BIND 9.x STIG, Version 1, Release 2

**V-72407**

Added "allow-recursion {none;};" to the check and fix statements.

**V-72409**

Adjusted the check and fix statements to use "notify explicit" and "also-notify".

**V-72421**

Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72443**

Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72445**

Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72447**

Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72449**

Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72451**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72453**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72455**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72457**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72459**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72461**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72469**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72471**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72473**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72477**
Adjusted the check and fix to allow for file ownership by the named process account.

**V-72495**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72497**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**V-72503**
Adjusted BIND DNSSEC requirement to state DNSSEC is not required on SIPRNet.

**Documentation Update**
Adjusted the Overview document to state DNSSEC is not required on SIPRNet.

## BIND DNS STIG, Version 4, Release 1-20

**V-74655**

Added requirement for verifying BIND DNS version 9.x or greater. Sunset STIG due to release of BIND DNS 9.x STIG.

## BlackBerry BES 12.3.x MDM STIG, Version 1, Release 3

**V-68685**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68687**

Intent of requirement clarified in Vulnerability Discussion

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68689**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68691**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68693**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68695**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68697**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68703**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

**V-68705**

In the previous release of this STIG all of the checks were incorrectly targeted; the STIG was previously called BB BES 12-3x MDM and the name was changed to BB BES 12-5x MDM, added the BES 12.5 target to each check.

## Database SRG, Version 2, Release 7

**V-61407**

Made the 365-day maximum password lifetime for non-interactive accounts explicit.

## Desktop Applications General STIG, Version 4, Release 5

**Documentation Update**

Modified Overview to reflect STIG is no longer applicable due to requirements having been migrated to other STIGs. STIG will be Sunsetted.

## DoD Internet-NIPRNet DMZ Technology Device STIG, Version 3, Release 4

**Documentation Update**

Updated release number.

## DoD Internet-NIPRNet DMZ Technology Policy STIG, Version 3, Release 4

**V-14910**

Updated Rule Title to include "Phyiscal or Virtual".

## ESRI ArcGIS for Server 10.3 STIG , Version 1, Release 2

**Documentation Update**

Update Overview document to include a revised scope statement that states the STIG applies to Windows/IIS versions only.

## Exchange 2010 Mailbox Server STIG, Version 1, Release 10

**V-33625**

Added check content to allow for certain applications to reside on same partition as Exchange.

## F5 BIG-IP Device Management 11.x STIG, Version 1, Release 5

**V-60163**

Corrected Check Content to change "SSL" to "Encryption".

## Google Chrome Browser STIG, Version 1, Release 9

**V-44737**

This policy will only display in the chrome://policy tab on domain joined systems. On standalone systems, the policy will not display. The value in the Group Policy editor and the registry will be present, as specified in the STIG, on standalone and domain joined systems. The STIG does not have any

**V-44741**

The STIG says the Group Policy name is "Enable the password manager" but the new admin templates show a policy name of "Enable saving passwords to the password manager".

**V-44771**

This policy will only display in the chrome://policy tab on domain joined systems. On standalone systems, the policy will not display. The value in the Group Policy editor and the registry will be present, as specified in the STIG, on standalone and domain joined systems. The STIG does not have any

**V-44781**
Remove requirement due to deprecated policy setting.

**V-44783**
Remove requirement due to deprecated policy setting.

**V-75165**
Add a blacklist check for chrome://history.

## Google Chrome for Windows Benchmark, Version 1, Release 4

**V-44781**
Remove requirement due to deprecated policy setting.

**V-75165**
Added OVAL to check for chrome://history in URLBlacklist.

## HBSS ePO 5.x STIG, Version 1, Release 13

**V-15354**
Modified check and fix text to require latest FIPS 140-x version.

**V-17890**
Modified check content to validate dashboard refresh rate for dashboards for all users.

**V-24169**
Added check criteria be an automatic open finding if V-14507 is an open finding.

**V-31358**
Added "nosa (disabled)" account to the exception list.

**V-43190**
Removed Note about ACCM being a preferred scanner due to OPORD requirement of ACCM Audits.

**V-43194**
Added check criteria to verify frequency of APS frequency in accordance to OPORD.

## HBSS HIP 8 Firewall STIG, Version 1, Release 9

**V-47481**
Added additional criteria to require firewall must be enabled.

**V-47485**
Modified check content to review the related ePO policy firewall rule policy rather than in the desktop GUI.

**V-47487**
Modified check content for clarity and ease of validating.

## HBSS McAfee Agent STIG, Version 4, Release 14

**V-14529**

Modified check criteria to accurately reflect option to select as "Repository list selection - Use this repository list".

**V-43051**

Removed Note about ACCM being a preferred scanner due to OPORD requirement of ACCM Audits.

**V-66969**

Missed in XCCDF Manual benchmark for April; ensured included in release.

**V-73125**

Modified check content to reflect similar verbiage as OPORD.

**V-75317**

Added requirement for APS to be installed on each endpoint.

## HBSS Remote Console STIG, Version 4, Release 14

**V-14514**

Modified check to clarify requirement is N/A for systems which are only accessing via the WEB GUI. Modified Severity downgrade guidance based upon the above.

## HBSS Rogue Sensor STIG, Version 4, Release 9

**V-14500**

Modified check and fix content to reflect current OPORD references.

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

**V-70483**

Updated the requirement to allow for documented use of the Remote Copy feature to meet mission objectives.

**V-70485**

Updated the requirement to allow for documented use of the CIM management client to meet mission objectives.

**V-70501**

Added “3parcimuser” to the list of allowed users.

**V-74657**

Added a requirement for the use of an encryption device when the Remote Copy feature is being used.

**V-74659**

Added a requirement for the use of encryption when the CIM management client is being used.

**Documentation Update**

Added the “3parcimuser” to section 2.1 as a vendor-recommended account name.

## HP-UX 11.31 STIG, Version 1, Release 14

**V-4083**

Added an applicability statement for systems that do not have graphical desktop environments.

**V-12006**

Updated the check to look at the helpfile instead of using the telnet application and command.

**V-22413**

Updated the check and fix to allow for "all" and "from any to any" as acceptable rule options.

**V-22414**

Updated the check and fix to allow for "all" and "from any to any" as acceptable rule options.

## IIS 7.0 STIG, Version 1, Release 14

**V-2230**

Include a specific reference to perform the check only within the IIS Root/Website directories.

**V-2240**

The "check content" section contains two errors. Step 2 tells users to cd into the "\windows\system32\inetserv" directory, but "inetserv" is a typo. It should say "inetsrv". Step 3 tells users to enter "appcmd list config /section:system.applicationH

## Infoblox 7.x DNS STIG, Version 1, Release 4

**V-68523**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68525**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68527**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68531**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68533**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68535**

Modified check content for DNSSEC requirement to be N/A on a Classified network.
Modified requirement and check content to reflect KSK rollover.

**V-68537**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68539**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68547**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68557**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68559**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68561**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68571**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68573**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68575**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68577**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68579**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68581**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68583**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68585**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68587**
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68597**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68599**

Modified check content for DNSSEC requirement to be N/A on a Classified network.
Modified requirement and check content to reflect ZSK rollover.
Modified requirement to also validate signature validity.

**V-68601**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68607**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68609**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68619**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68635**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-68701**

Modified check content for DNSSEC requirement to be N/A on a Classified network.

## Internet Explorer 11 Benchmark, Version 1, Release 10

**V-46473**

Created new OVAL for the existing STIG requirement.

**V-64729**

Added new OVAL content for the requirement as the requirement has been modified to address the HKLM registry hive in lieu of the HKCU registry hive.

**V-75169**

Created new OVAL for the new STIG requirement.

**V-75171**

Created new OVAL for the new STIG requirement.

## Intrusion Detection and Prevention System (IDPS) SRG, Version 2, Release 3

**V-55347**

Change pattern recognition pre-processors to anomaly detection to less vendor-specific terminology.

## Joint Information Environment (JIE) Core Data Center (CDC) STIG, Version 2

**V-59245**

CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59445**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59447**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59449**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59455**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59457**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59459**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59465**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59469**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59471**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59485**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-73827**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

## Joint Information Environment (JIE) Installation Processing Node (IPN) STIG

**V-59243**

CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59381**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59383**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59385**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59391**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59393**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59395**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59401**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59407**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59409**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

**V-59423**
CCI mappings are CDS specific. Change CCI-002213 to CCI-002415 for logical separation. Delete CCI-2216.

## Juniper SRX SG IDPS STIG, Version 1, Release 2

**V-66421**
Change pattern recognition pre-processors to anomaly detection to change from Cisco SNORT based terminology.

## Mainframe Product SRG, Version 1, Release 2

**V-68513**

Correct typo in Vul discussion to "non-privilege" users.

## McAfee VirusScan 8.8 Managed Client STIG, Version 5, Release 17

**Documentation Update**

Modified Overview document to reflect local VirusScan console is not an approved method for validating ePO deployed configuration settings.

## Microsoft .Net Framework 4.0 STIG, Version 1, Release 4

**V-7063**

MS .Net Framework 4.0 path issue. .NET 4.0 STIG should read:
For 64 bit systems, caspol.exe is located at
%SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319.
It currently states:
%SYSTEMROOT%\Microsoft.NET64\Framework\v4.0.30319.

**V-7067**

MS .Net Framework 4.0 path issue. .NET 4.0 STIG should read:
For 64 bit systems, caspol.exe is located at
%SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319.
It currently states:
%SYSTEMROOT%\Microsoft.NET64\Framework\v4.0.30319.

## Microsoft Internet Explorer 11 STIG, Version 1, Release 13

**V-46473**

"SecureProtocols" is REG_DWORD = 2560.

**V-75169**

"Allow VBScript to run in Internet Explorer" must be "Enabled".

**V-75171**

"Allow VBScript to run in Internet Explorer" must be "Enabled".

## Microsoft Office Outlook 2016 Benchmark, Version 1, Release 2

**V-71137**

Removed requirement at DoD consensus request.

**V-71269**

Removed requirement at DoD consensus request.

**V-71279**

Removed requirement at DoD consensus request.

## Microsoft Office Project 2013 Benchmark, Version 1, Release 4

**V-40891**

Disabled Rule in OVAL corresponding to removal in STIG.

## Microsoft Office System 2010 STIG, Version 1, Release 11

**V-17561**

Removed requirement for disabling of .png output format.

## Microsoft Office System 2013 STIG, Version 1, Release 5

**V-17561**

Removed requirement for disabling of .png output format.

**V-17759**

Corrected Administrative Template directive.

**V-40881**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

**V-40882**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

**V-40883**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

**V-40884**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

**V-40885**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

**V-40886**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

**V-40887**

Modified check content to reflect validation to be made in HKU vs HKCU registry keys.

## Microsoft Outlook 2016 STIG, Version 1, Release 2

**V-71137**

Removed requirement at DoD consensus request.

**V-71269**

Removed requirement at DoD consensus request.

**V-71279**

Removed requirement at DoD consensus request.

## Microsoft Project 2013 STIG, Version 1, Release 3

**V-40891**

Removed requirement as was removed from other Office 2013 products.

## Microsoft Windows 2012 Server DNS STIG, Version 1, Release 7

**V-58557**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58575**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58589**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58591**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58599**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58601**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58631**

Modified check content to allow Dynamic updates to also be set to "none".

**V-58639**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58647**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58651**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58653**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58657**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58659**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58663**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58665**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58667**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58669**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58671**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58673**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58675**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58677**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58679**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58681**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58683**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58687**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58689**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58701**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58703**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.

Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58705**

Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

**V-58717**
Modified check content for DNSSEC requirement to be N/A in a solely AD-integrated DNS environment supporting only AD zones.
Modified check content for DNSSEC requirement to be N/A on a Classified network.

## MobileIron Core v9.x MDM STIG, Version 1, Release 3

**Documentation Update**
Supplemental document updated with new PKI information.

## Mozilla Firefox STIG, Version 4, Release 19

**V-6318**
"security.enterprise_roots.enabled" Boolean True (adds DoD cert compatibility);
"plugin.load_flash_only" Boolean False (allows Java/Silverlight/Acrobat to continue working).

**V-15777**
"privacy.sanitize.timeSpan" should be "4".
"privacy.sanitize.promptOnSanitize" depreciated.
The setting "privacy.sanitize.sanitizeOnShutdown" is not discussed.

**V-19743**
"privacy.sanitize.promptOnSanitize" depreciated.

**V-57681**
57681 appears to be a new check, but is not annotated in the history.

## MS Office System 2010 Benchmark, Version 1, Release 3

**V-17561**
Disabled the rule in OVAL benchmark in conjunction with the removal of the requirement from the manual STIG.

## MS Office System 2013 Benchmark, Version 1, Release 4

**V-17561**
Disabled the rule in OVAL benchmark in conjunction with the removal of the requirement from the manual STIG.

## MS SQL Server 2012 Database STIG, Version 1, Release 15

**V-40911**
Moved to Database STIG from Instance STIG.

**V-41420**
Wording modified to clarify responsibility for determining whether to encrypt.

## MS SQL Server 2012 Instance STIG, Version 1, Release 15

**V-40911**

Moved to Database STIG from Instance STIG.

**V-40946**

Check: slight rewording for clarity.

**V-40952**

Modified Check and Fix wording to clarify that additional permissions are OK if documented and authorized. Added Notes 1 and 2 to Check.

**V-40953**

Modified Check and Fix wording to clarify that additional permissions are OK if documented and authorized. Added Notes 1 and 2 to Check.

**V-41016**

Modified Check and Fix wording to clarify that additional permissions are OK if documented and authorized. Added Notes 1 and 2 to Check.

**V-72415**

Made the 365-day maximum password lifetime for non-interactive accounts explicit.

**Documentation Update**

Provided an outline of how to use a SQL Server Audit instead of Trace.

## MS SQL Server 2014 Database STIG, Version 1, Release 5

**V-67877**

Moved to Database STIG from Instance STIG.

## MS SQL Server 2014 Instance STIG, Version 1, Release 6

**V-67789**

Modified Check and Fix wording to clarify that additional permissions are OK if documented and authorized.

**V-67791**

Modified Check and Fix wording to clarify that additional permissions are OK if documented and authorized.

**V-67793**

Modified Check and Fix wording to clarify that additional permissions are OK if documented and authorized.

**V-67813**

Check: slight rewording for clarity. Changed severity to Category III.

**V-67877**

Moved to Database STIG from Instance STIG.

**V-67945**

Made the 365-day maximum password lifetime for non-interactive accounts explicit.

## Multifunction Device and Network Printers STIG, Version 2, Release 10

**V-6778**

Check did not address a vulnerability or provide any security advantage.

## Network Device Management (NDM) SRG, Version 2, Release 11

**V-55153**

Update to state that NIST CMVP validation is required. Only utilizing FIPS 140-2 compliant algorithms is not sufficient; CMVP validation is required by law.

**V-55265**

Include the requirement to use FIPS-140-2 for SSH encryption and HMAC.

**V-64001**

Add the following text to the vulnerability discussion: Safe be opened periodically and audited for presence and that the envelope had not been opened. The signature of the auditor and the date of the audit should be added to the envelop as a record. Add text to secure the shared secret, userid, and

## Network Firewall STIG - Cisco, Version 8, Release 23

**V-3069**

Updated Check Content section example.

**Documentation Update**

Updated release number.

## Network Infrastructure L3 Switch STIG - Cisco, Version 8, Release 23

**V-3069**

Updated Check Content section example.

**Documentation Update**

Updated release number.

## Network Infrastructure Router STIG - Cisco, Version 8, Release 23

**V-3069**

Updated Check Content section example.

## Network Infrastructure Router STIG - Juniper, Version 8, Release 23

**V-3069**

Updated Check Content section example.

## Network Infrastructure Router STIG, Version 8, Release 23

**Documentation Update**
Updated release number.

## Network Layer 2 Switch STIG - Cisco, Version 8, Release 21

**V-3069**
Updated Check Content section example.

**Documentation Update**
Updated release number.

## Network Perimeter L3 Switch STIG - Cisco, Version 8, Release 26

**V-3069**
Updated Check Content section example.

**Documentation Update**
Updated release number.

## Network Perimeter Router STIG - Cisco, Version 8, Release 26

**V-3069**
Updated Check Content section example.

## Network Perimeter Router STIG - Juniper, Version 8, Release 26

**V-14671**
Updated Check Content section example.

## Network Perimeter Router STIG, Version 8, Release 26

**Documentation Update**
Updated release number.

## Oracle Database 11.2g STIG, Version 1, Release 12

**V-52159**
Linked requirement to a second CCI.

**V-52361**
Wording modified to acknowledge the limits of auditing the disabling of accounts.

**V-52469**
Wording modified to acknowledge the limits of auditing the disabling of accounts.

**V-53967**
Modified rule title to make the requirement compatible with cloud computing.

**V-54003**
Wording modified to require obfuscation before data transfer, rather than after.

**V-75031**
Replaces V-52261, which was accidentally deleted.

## Oracle Database 11g Installation STIG, Version 8, Release 20

**V-57611**
Modified rule title to make the requirement compatible with cloud computing. Reduced Severity to Category III.

## Oracle Database 11g Instance STIG, Version 8, Release 20

**V-3819**
Wording modified to require obfuscation before data transfer, rather than after.

## Oracle Database 12c STIG, Version 1, Release 8

**V-61417**
Modified rule title to make the requirement compatible with cloud computing.

**V-61453**
Wording modified to require obfuscation before data transfer, rather than after.

**V-61571**
Wording modified to acknowledge the limits of auditing the disabling of accounts.

**V-61625**
Wording modified to acknowledge the limits of auditing the disabling of accounts.

**V-61643**
Linked requirement to a second CCI.

## Oracle JRE 8 Windows STIG, Version 1, Release 4

**V-66939**
A ghost entry exists without a vulid.
Add C:\Windows\Sun…. as an additional location.

**V-66941**
Add C:\Windows\Sun…. as an additional location.

**V-66943**
Add C:\Windows\Sun…. as an additional location.

**V-66945**
Add C:\Windows\Sun…. as an additional location.

**V-66947**
Add C:\Windows\Sun…. as an additional location.

**V-66949**
Add C:\Windows\Sun…. as an additional location.

**V-66951**
Add C:\Windows\Sun…. as an additional location.

**V-66953**
Add C:\Windows\Sun…. as an additional location.

**V-66955**
Add C:\Windows\Sun…. as an additional location.

**V-66957**
Add C:\Windows\Sun…. as an additional location.

**V-66961**
Add C:\Windows\Sun…. as an additional location.

**V-66963**
Add C:\Windows\Sun…. as an additional location.

## Oracle Linux 5 STIG, Version 1, Release 11

**V-22569**
Updated check content with TLS Certificate directives in the LDAP config file.

## Palo Alto Networks ALG STIG, Version 1, Release 3

**V-62549**
Update fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.

**V-62551**
Update fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.

**V-62553**
Update fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.

**V-62633**
Update fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.

**V-62635**
Update fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.

## Palo Alto Networks NDM STIG, Version 1, Release 3

**V-62721**

Update fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.

## Red Hat 6 Benchmark, Version 1, Release 16

**V-38438**

Updated OVAL to include /boot/efi/EFI/redhat/grub.conf in check.

**V-38583**

Updated OVAL to include /boot/efi/EFI/redhat/grub.conf in check.

**V-38585**

Updated OVAL to include /boot/efi/EFI/redhat/grub.conf in check.

**V-38635**

Removed OVAL as adjtimex auditing requirement is being removed from the manual STIG.

**V-38658**

Updated OVAL to check the PAM configuration in accordance with the manual STIG update.

## Red Hat 6 STIG, Version 1, Release 16

**V-38438**

Added UEFI information to the check and fix statements.

**V-38583**

Added UEFI information to the check and fix statements.

**V-38585**

Added UEFI information to the check and fix statements.

**V-38635**

Removed the requirement as there is not an adjtimex in hwclock, and it has not been replaced with another command.

**V-38658**

Added "requisite" as an acceptable option for use with pam_pwhistory.so.

## Red Hat Enterprise Linux 7 STIG, Version 1, Release 2

**V-71891**

Removed items from Fix instructions that were not exclusive to screen lock.

**V-71893**

Removed items from Fix instructions that were not exclusive to idle delay.

**V-71905**

Wrote new Fix section to meet the requirement text for password complexity.

**V-71961**
Updated grep command in Check instructions.

**V-71983**
Updated Check and Fix instructions to blacklist USB devices using the blacklist.conf file.

**V-72017**
Removed extra space from the command in the Check content.

**V-72019**
Removed extra space from the command in the Check content.

**V-72021**
Removed extra space from the command in the Check content.

**V-72047**
Updated find command in Check content.

**V-72053**
Removed extra space from the command in the Check content.

**V-72063**
Updated entire Check content to fit the requirement.

**V-72095**
Updated code in Fix content.

**V-72181**
Removed requirement due to differences in package availability in standard installation.

**V-72239**
Updated Check and Fix content to require the value "no".

**V-72271**
Updated command and instructions in Fix content.

**V-72275**
Updated Check content to better address SSHD configuration.

**V-73173**
Updated the path used in bot the Check and Fix instructions.

## Removable Storage and External Connections STIG, Version 1, Release 6

**V-22111**

Removed outdated reference to DAR contract and move content from the Check Content section to the Discussion section.

**V-22113**

Removed non-applicable requirement from the check content section.

**V-22177**

Updated multiple issues with the Rule Title, Check Content, and Fix Text sections.

## SLES V11 for System Z STIG, Version 1, Release 10

**V-22569**

Updated check content with TLS Certificate directives in the LDAP config file.

## Solaris 10 SPARC Benchmark, Version 1, Release 18

**V-22304**

Updated OVAL to check password hash algorithms in accordance with the manual STIG update.

## Solaris 10 SPARC STIG, Version 1, Release 19

**V-22303**

Updated Check and Fix instructions to whitelist hashing algorithms.

**V-22304**

Updated Check and Fix instructions to whitelist hashing algorithms.

## Solaris 10 X86 Benchmark, Version 1, Release 18

**V-22304**

Updated OVAL to check password hash algorithms in accordance with the manual STIG update.

## Solaris 10 X86 STIG, Version 1, Release 19

**V-22303**

Updated Check and Fix instructions to whitelist hashing algorithms.

**V-22304**

Updated Check and Fix instructions to whitelist hashing algorithms.

## Solaris 11 SPARC Benchmark, Version 1, Release 7

**V-48025**

Disabled the OVAL since the updated check requires the use of sxadm, which OVAL does not currently support.

## Solaris 11 SPARC STIG, Version 1, Release 12

**V-48025**

Updated Check and Fix instructions due to changes in Solaris 11.3.

**V-48187**

Updated Group Title and Vulnerability Discussion to reflect new methods of tracking multiple SRG IDs.

**V-72827**
Updated Group Title.

## Solaris 11 X86 Benchmark, Version 1, Release 7

**V-48001**
Updated the OVAL to match the updated STIG requirement check and fix text.

**V-48025**
Disabled the OVAL since the updated check requires the use of sxadm, which OVAL does not currently support.

## Solaris 11 X86 STIG, Version 1, Release 12

**V-48001**
Updated Check and Fix instructions to use a custom configuration file for GRUB.

**V-48025**
Updated Check and Fix instructions due to changes in Solaris 11.3.

**V-48187**

Updated Group Title and Vulnerability Discussion to reflect new methods of tracking multiple SRG IDs.

**V-72827**
Updated Group Title.

## VMware ESXi Version 5 Virtual Machine STIG, Version 1, Release 7

**V-39490**
Updated CCI list.

## VMware vSphere ESXi 6.0 STIG, Version 1, Release 3

**V-63553**
Removed requirement as it can be collapsed into ESXI-06-200035.

**V-63885**
Updated CCI list.

## VMware vSphere vCenter Server Version 6 STIG, Version 1, Release 4

**V-63951**
Updated CCI mapping.

**V-64007**

Updated Check instructions related to permissions related to vCenter database administrator role.

## Windows 2008 DC Benchmark, Version 6, Release 39

**V-1098**

Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**

Added OVAL to check permissions on Winreg registry key.

**V-26070**

Added OVAL to check permissions on Winlogon registry key.

## Windows 2008 DC STIG, Version 6, Release 37

**V-1098**

Updated reset account lockout counter to 15 minutes or greater.

**V-1099**

Updated account lockout duration to 15 minutes or greater.

**V-1120**

Updated Check to more accurately verify FTP configuration.

**V-1121**

Updated Check to more accurately verify FTP configuration.

**V-3337**

Removed exception note, no longer applicable.

**V-14243**

Updated Rule Title to more accurately reflect requirement.

**V-26602**

Clarified Rule Title, service must be disabled unless required.

**V-36451**

Clarified requirement - policy required at minimum, technical means can be used to enforce.

## Windows 2008 MS Benchmark, Version 6, Release 39

**V-1098**

Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**

Added OVAL to check permissions on Winreg registry key.

**V-26070**

Added OVAL to check permissions on Winlogon registry key.

## Windows 2008 MS STIG, Version 6, Release 37

**V-1098**

Updated reset account lockout counter to 15 minutes or greater.

**V-1099**

Updated account lockout duration to 15 minutes or greater.

**V-1120**

Updated Check to more accurately verify FTP configuration.

**V-1121**

Updated Check to more accurately verify FTP configuration.

**V-3337**

Removed exception note, no longer applicable.

**V-14243**

Updated Rule Title to more accurately reflect requirement.

**V-26602**

Clarified Rule Title, service must be disabled unless required.

**V-36451**

Clarified requirement - policy required at minimum, technical means can be used to enforce.

## Windows 2008 R2 DC Benchmark, Version 1, Release 25

**V-1098**

Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**
Added OVAL to check permissions on Winreg registry key.

**V-26070**
Added OVAL to check permissions on Winlogon registry key.

## Windows 2008 R2 DC STIG, Version 1, Release 23

**V-1098**
Updated reset account lockout counter to 15 minutes or greater.

**V-1099**
Updated account lockout duration to 15 minutes or greater.

**V-1112**
Corrected typo referring to built-in admin account as disabled.

**V-1120**
Updated Check to more accurately verify FTP configuration.

**V-1121**
Updated Check to more accurately verify FTP configuration.

**V-3337**
Removed exception note, no longer applicable.

**V-14243**
Updated Rule Title to more accurately reflect requirement.

**V-26602**
Clarified Rule Title, service must be disabled unless required.

**V-36451**
Clarified requirement - policy required at minimum, technical means can be used to enforce.

## Windows 2008 R2 MS Benchmark, Version 1, Release 26

**V-1098**
Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**
Added OVAL to check permissions on Winreg registry key.

**V-26070**
Added OVAL to check permissions on Winlogon registry key.

## Windows 2008 R2 MS STIG, Version 1, Release 23

**V-1098**
Updated reset account lockout counter to 15 minutes or greater.

**V-1099**
Updated account lockout duration to 15 minutes or greater.

**V-1112**
Corrected typo referring to built-in admin account as disabled.

**V-1120**
Updated Check to more accurately verify FTP configuration.

**V-1121**
Updated Check to more accurately verify FTP configuration.

**V-3337**
Removed exception note, no longer applicable.

**V-14243**
Updated Rule Title to more accurately reflect requirement.

**V-26602**
Clarified Rule Title, service must be disabled unless required.

**V-36439**
Updated Fix to use custom admin template instead of direct registry update.

**V-36451**
Clarified requirement - policy required at minimum, technical means can be used to enforce.

## Windows 2012/2012 R2 DC Benchmark, Version 2, Release 9

**V-1081**
Updated OVAL to reflect STIG changes that allow for ReFS

**V-1098**
Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**
Added OVAL to check permissions on Winreg registry key.

**V-26070**
Added OVAL to check permissions on Winlogon registry key.

**V-26580**
Updated the OVAL content to only allow Security Log maximum size to be 196608 KB or more.

## Windows 2012/2012 R2 DC STIG, Version 2, Release 9

**V-1081**
Updated to include ReFS as an acceptable disk format.

**V-1098**
Updated reset account lockout counter to 15 minutes or greater.

**V-1099**
Updated account lockout duration to 15 minutes or greater.

**V-1112**
Corrected typo referring to built-in admin account as disabled.

**V-1120**
Updated Check to more accurately verify FTP configuration.

**V-1121**
Updated Check to more accurately verify FTP configuration.

**V-14243**
Updated Rule Title to more accurately reflect requirement.

**V-26602**
Clarified Rule Title, service must be disabled unless required.

**V-36451**
Clarified requirement - policy required at minimum, technical means can be used to enforce.

## Windows 2012/2012 R2 MS Benchmark, Version 2, Release 9

**V-1081**
Updated OVAL to reflect STIG changes that allow for ReFS

**V-1098**

Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**

Added OVAL to check permissions on Winreg registry key.

**V-26070**

Added OVAL to check permissions on Winlogon registry key.

**V-26580**

Updated the OVAL content to only allow Security Log maximum size to be 196608 KB or more.

## Windows 2012/2012 R2 MS STIG, Version 2, Release 9

**V-1081**

Updated to include ReFS as an acceptable disk format.

**V-1098**

Updated reset account lockout counter to 15 minutes or greater.

**V-1099**

Updated account lockout duration to 15 minutes or greater.

**V-1112**

Corrected typo referring to built-in admin account as disabled.

**V-1120**

Updated Check to more accurately verify FTP configuration.

**V-1121**

Updated Check to more accurately verify FTP configuration.

**V-14243**

Updated Rule Title to more accurately reflect requirement.

**V-26602**

Clarified Rule Title, service must be disabled unless required.

**V-36439**

Updated Fix to use custom admin template instead of direct registry update.

**V-36451**

Clarified requirement - policy required at minimum, technical means can be used to enforce.

## Windows 7 Benchmark, Version 1, Release 33

**V-1098**

Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**

Enabled Winreg registry check previously disabled due to an SCC bug.

**V-26070**

Added OVAL to check permissions on Winlogon registry key.

## Windows 7 STIG, Version 1, Release 27

**V-1098**

Updated reset account lockout counter to 15 minutes or greater.

**V-1099**

Updated account lockout duration to 15 minutes or greater.

**V-36439**

Updated Fix to use custom admin template instead of direct registry update.

## Windows 8/8.1 Benchmark, Version 1, Release 19

**V-1098**

Updated the OVAL content to allow for the period of time before the bad logon counter is reset to be configured to 15 minutes or greater.

**V-1099**

Updated the OVAL content to allow for the period of time before the account lockout duration to be configured to 15 minutes or greater or to only allow the account to be unlocked by an administrator.

**V-1152**

Enabled Winreg registry check previously disabled due to an SCC bug.

**V-26070**

Added OVAL to check permissions on Winlogon registry key.

**V-26470**

Updated the OVAL content to use an OVAL definition independent of the definition used by the Windows 10 benchmark for the "Access this computer from the network" user right requirement.

**V-32282**
Enabled Winreg registry check previously disabled due to an SCC bug.

## Windows 8/8.1 STIG, Version 1, Release 18

**V-1099**
Updated account lockout duration to 15 minutes or greater.

**V-36770**
Updated Fix to use custom admin template instead of direct registry update.

**V-68687**
Updated reset account lockout counter to 15 minutes or greater.

## Windows Server 2016 Benchmark, Version 1, Release 2

**V-73309**
Repackaged benchmark due to manual STIG update.

## Windows Server 2016 STIG, Version 1, Release 2

**V-73223**
Corrected typo in command used to verify requirement on member servers.

**V-73231**
Corrected typo in command used to verify requirement on member servers.

**V-73261**
Updated member server query to filter for local accounts only.

**V-73263**
Updated member server query to filter for local accounts only.

**V-73309**
Updated account lockout duration to 15 minutes or greater.

## z/OS BMC MAINVIEW for z/OS for ACF2 STIG , Version 6, Release 8

**Documentation Update**
Add new mainview resources for mainview CICS  to Addendum.

## z/OS BMC MAINVIEW for z/OS for RACF STIG , Version 6, Release 8

**Documentation Update**
Add new mainview resources for mainview CICS  to Addendum.

## z/OS BMC MAINVIEW for z/OS for TSS STIG , Version 6, Release 8

**Documentation Update**

Add new mainview resources for mainview CICS  to Addendum.

## z/OS CA 1 Tape Management for ACF2 STIG , Version 6, Release 7

**Documentation Update**

Add group for off-site librarians IN THE Addendum for  ZCA10020.

## z/OS CA 1 Tape Management for RACF STIG , Version 6, Release 7

**Documentation Update**

Add group for off-site librarians IN THE Addendum for  ZCA10020.

## z/OS CA 1 Tape Management for TSS STIG , Version 6, Release 7

**Documentation Update**

Add group for off-site librarians IN THE Addendum for  ZCA10020.

## z/OS CL/SuperSession for ACF2 STIG , Version 6, Release 9

**V-16932**

Update the FIX to remove specific Data set names.

**V-17067**

Update the FIX to remove specific Data set names.

## z/OS CL/SuperSession for RACF STIG , Version 6, Release 9

**V-16932**

Update the FIX to remove specific Data set names.

**V-17067**

Update the FIX to remove specific Data set names.

## z/OS CL/SuperSession for TSS STIG , Version 6, Release 9

**V-16932**

Update the FIX to remove specific Data set names.

**V-17067**

Update the FIX to remove specific Data set names.

## z/OS Cross Ref of SRRAUDIT spreadsheet, Version 6, Release 32

**V-7482**

Changed spreadsheet adding new resources and the access requirements identified in ticket.

**V-17947**

Changed spreadsheet adding new resources and the access requirements identified in ticket.
Changed spreadsheet adding new requirements identified in ticket.

**V-21592**

Changed spreadsheet adding UPDATE and CONTROL to access requirements that specify CONTROL as documented in ticket.

## z/OS CSSMTP for ACF2 STIG , Version 6, Release 4

**V-17067**

Create new vulnerability for the CSSMTP Checkpoint dataset.

## z/OS CSSMTP for RACF STIG , Version 6, Release 4

**V-17067**

Create new vulnerability for the CSSMTP Checkpoint dataset.

## z/OS CSSMTP for TSS STIG , Version 6, Release 4

**V-17067**

Create new vulnerability for the CSSMTP Checkpoint dataset.

## z/OS SRR Scripts, Version 6, Release 32

**V-71203**

Changed scripts to correct error that was documented in ticket.

**SRR Script Update**

Changed scripts to correct error that was documented in ticket.
Changes to JCL in CARJ0002 SPACE allocation for TEMP5.

## zOS ACF2 STIG, Version 6, Release 32

**V-6993**

Delete ZUSS0050.

**V-7050**

Update ZUSS0048 to reflect using the BPX.UNIQUE.USER resource as well as other modeling userid for USS and having it properly defined. And BPX.NEXT.USER be properly defined if automatic generation of UIDs and GIDs is being used where required.

**V-7482**

Change ACP00282 and the z/OS STIG Addendum to add new resources identified in z/OS V2R1.0 MVS System Commands and z/OS V2R2.0 MVS System Commands.

**Documentation Update**

Update resources in Addendum with new SDSF panels that are protectable via the security product.

## zOS RACF STIG, Version 6, Release 32

**V-298**

Update RACF0760 to Audit ALL(READ).

**V-6997**

Delete ZUSS0050.

**V-7050**

Update ZUSS0048 to reflect using the BPX.UNIQUE.USER resource as well as other modeling userid for USS and having it properly defined. And BPX.NEXT.USER be properly defined if automatic generation of UIDs and GIDs is being used where required.

**V-7482**

Change ACP00282 and the z/OS STIG Addendum to add new resources identified in z/OS V2R1.0 MVS System Commands and z/OS V2R2.0 MVS System Commands.

**V-75057**

Add requirement for TCP/IP "For TCP/IP the SERVAUTH CLASS must be active.

**V-75059**

Add new vulnerability to address RACF Global access tracking.

**Documentation Update**

Update resources in Addendum with new SDSF panels that are protectable via the security product.

## zOS TSS STIG, Version 6, Release 32

**V-7000**

Delete ZUSS0050.

**V-7050**

Update ZUSS0048 to reflect using the BPX.UNIQUE.USER resource as well as other modeling userid for USS and having it properly defined. And BPX.NEXT.USER be properly defined if automatic generation of UIDs and GIDs is being used where required.

**V-7482**

Change ACP00282 and the z/OS STIG Addendum to add new resources identified in z/OS V2R1.0 MVS Svstem Commands and z/OS V2R2.0 MVS Svstem Commands.

**Documentation Update**

Update resources in Addendum with new SDSF panels that are protectable via the security product. Change access level for TSS Abendaid User datasets in the Addendum from Access(Control) to Access(Update, Control).