JANUARY 2018 MAINTENANCE RELEASE: STIGS TO BE RELEASED

Active Directory Domain STIG, Version 2, Release 9

V-36438

Clarified use of LAPS and all local administrator accounts must be addressed.

V-78131

Added requirement for domain level admin accounts to be members of the Protected Users group.

Adobe Acrobat Pro XI STIG, Version 1, Release 2

V-79057

Add CAT 1 finding for EOL Oct 15, 2017.

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

V-65799

Swap the rule titles between: ARDC-CL-000310 and ARDC-CL-000320.
ARDC-CL-000310 NEW: Adobe Reader DC must disable the ability to elevate IE Trusts to Privileged Locations.

V-65803

Swap the rule titles between: ARDC-CL-000310 and ARDC-CL-000320.
ARDC-CL-000320 NEW: Adobe Reader DC must disable the ability to specify Host-Based Privileged Locations.

Documentation Update

Need to add the attached adm/admx template files to the Adobe Acrobat DC Continuous and Classic STIGS. These template files are used to create GPO menu options to secure the product. Create a template folder in the STIG zip file.

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

Benchmark Update

Repackaged benchmark to accommodate manual STIG updates.

Adobe Acrobat Reader DC Continuous STIG, Version 1, Release 3

Documentation Update

Need to add the attached adm/admx template files to the Adobe Acrobat DC Continuous and Classic STIGS. These template files are used to create GPO menu options to secure the product. Create a template folder in the STIG zip file.

Adobe ColdFusion 11 STIG, Version 1, Release 4

V-62479

Need to add exclusions to allow for commercially signed certs when accessing the vendors site such as when downloading patches.

AIX 6.1 STIG, Version 1, Release 11

V-11940

Updated requirement to show that AIX 6.1 has reached End of Support.

Apple OS X 10.11 STIG, Version 1, Release 6

V-79059

Added new CAT I for the use of non-secure FTP.

Documentation Update

Fix Calendar/Contacts in Overview of OS X 10.11.
Updated Overview document to permit APN.

Apple OS X 10.12 STIG, Version 1, Release 2

V-76037

Updated code in configuration profile.

V-76039

Updated code in configuration profile.

V-76041

Updated code in configuration profile.

V-76045

Updated code in configuration profile.

V-76047

Updated code in configuration profile.

V-76049

Updated code in configuration profile.

V-76071

Corrected command listed in the Fix instructions.

Documentation Update

Updated Overview document to permit APN.

Application Security and Development STIG, Version 4, Release 5

V-70415

Change CCI from CCI-001275 - The organization defines the activities which will trigger alerts to security personnel of inappropriate or unusual activities.
To:
CCI-001274 The organization employs automated mechanisms to alert security personnel of organization-defined inappropriate or unusual activities with security implications

Application Server SRG, Version 2, Release 3

V-57517

Update check: Whereas the CAC is the standard DoD authentication token, the PIV is the standard authentication token used by federal/civilian agencies.
If access to the application server is limited to DoD personnel accessing the system via CAC and PIV access is not warranted or allowed as per the system security plan, this requirement is NA.

Application SRG, Version 2, Release 0-7

V-26962

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-27015

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-44877

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-45253

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-45317

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45321

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45323

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45325

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45365

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45599

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-45603

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

BIND 9.x STIG, Version 1, Release 3

V-72409

Modified to be in concurrence with V-72411.

V-72503

Added note for N/A finding if using for internal, reserved IP space only.

BIND 9.x, Version 1, Release 3

V-72411

Modified to be in concurrence with V-72409.

BlackBerry Enterprise Server 5.x STIG, Version 2, Release 10

V-19191

Modify check to sunset STIG.

Documentation Update

Updated format of all STIG documents.

Database SRG, Version 2, Release 8

V-32534

Added not-a-finding statement to Check.

EDB Postgres Advanced Server STIG, Version 1, Release 4

V-68961

Added not-a-finding statement to Check.

Esri ArcGIS Server 10.3 STIG, Version 1, Release 3

V-65319

Update check with vendor provided text.

V-65323

Update check and fix with vendor provided text.

V-65385

Update check and fix with vendor provided text.

V-65429

Update check and fix with vendor provided text.

V-65467

Update check with vendor provided text.

V-65477

Update check and fix with vendor provided text.

V-65499

Update check with vendor provided text.

V-65503

Update check with vendor provided text.

V-65509

Update check and fix with vendor provided text.

V-65515

Update check and fix with vendor provided text.

V-65517

Update check with vendor provided text.

Firewall STIG - Cisco, Version 8, Release 25

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

ForeScout CounterACT ALG STIG, Version 1, Release 2

V-76191

Add that 2 appliances configured for High Availability are also acceptable. Add the procedures from the vendor.

Good for Enterprise 8.x STIG, Version 1, Release 3

V-76677

Add exceptions to sunset requirement for sites with extended service agreements and end date for when exception is valid.

Google Chrome Browser STIG, Version 1, Release 11

V-44735

Add an NA for SIPR clause.

V-44769

DTBC-0025 Network Prediction must be disabled.
Change path name from ‘Do not predict network actions on any network connection’ to ‘Enable network prediction’.

V-44795

V44795 – DTBC-0040: Default behavior must block webpages from automatically running Flash plugin.
Vul Discussion: This policy allows you to set whether websites are allowed to automatically run the Flash plugin. Automatically running the Flash plugin can be either allowed for all websites or denied for all websites. If this policy is left not set, the user will be able to change this setting manually:
1 = Allow all sites to automatically run Flash plugin
2 = Block the Flash plugin
3 = Click to play
Fix Text: Windows group policy:
1. Open the group policy editor tool with gpedit.msc
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\
Policy Name: Default Flash setting
Policy State: Enabled
Policy Value: Click to play

V-52795

V52795 – DTBC-0051: URLs must be whitelisted for Flash plugin use.
Vul Discussion: This policy allows you to set a list of url patterns that specify sites which are allowed to run the Flash plugin. If this policy is left not set, the global default value will be used for all sites either from the ‘DefaultPluginsSetting’ policy if it is set, or the user’s personal configuration otherwise.
Fix Text: Windows group policy:
1. Open the group policy editor tool with gpedit.msc
2. Navigate to Policy Path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings
Policy Name: Allow the Flash plugin on these sites
Policy State: Enabled
Policy Value 1: *.mil

V-75165

Set new GPO "Enable deleting browser and download history" instead of using blacklist.

Google Chrome for Windows Benchmark, Version 1, Release 6

V-44769

Updated OVAL to account for STIG Changes.

V-44795

Updated OVAL to account for STIG Changes.

V-75165

Updated OVAL to account for STIG Changes.

HBSS Agent Handler Security STIG, Version 1, Release 10

V-14483

Modified check criteria regarding location of Agent Handler.

HBSS ePO 5.x STIG, Version 1, Release 14

V-14486

Added verbiage for other allowed IP addresses/protocols, generically and specifically to HBSS rollup/staging servers.

V-14495

Modified check criteria to include other ports and protocols to be configured.

V-14497

Expounded on Vulnerability Discussion and Check/Fix to refer to only ePO baselined applications and software.

V-15357

Modified check criteria to reflect current CYBERCOM directive references.

V-17882

Added HBSS2012 as a Target for the DoD WSUS configuration

V-24020

Added Note: If the ePO is not on a disconnected network, this check is NA to check criteria.

Modified to specify CRL folder location as per HBSS configuration guide.

V-51843

Modified check criteria to remove invalid URL reference.

HBSS HIP 8 Firewall STIG, Version 1, Release 10

V-47483

Modified check criteria to reflect allowed configuration of outbound traffic rules.

V-47485

Modified check criteria for clarity regarding IPv6 traffic.

V-47487

Modified check criteria to reflect allowed CAG/LAG rule configuration options.

HBSS HIP 8 STIG, Version 4, Release 20

V-14532

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14536

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14537

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14540

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14541

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14543

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14544

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14546

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14547

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14548

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-14560

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

Duplicate requirement of HIP 8 Firewall STIG requirement V47487. CAG/LAG rule belongs in HIP 8 Firewall STIG and not the HIP 8 STIG.

V-17891

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

Modified check criteria for clarity with validating signatures.

V-17893

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-31085

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-31086

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-43197

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-43199

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-43200

Modified check criteria to be specific to Rule Title regarding required IPS signatures.

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-43201

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-55659

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-55661

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-55663

Modified check procedure to more accurately reflect viewing effective policy on a managed asset.

V-72967

Modified check criteria for clarity with validating signatures.

HBSS McAfee Agent STIG, Version 4, Release 16

V-14526

Modified Fix text for correct verbiage.

HP-UX 11.31 STIG, Version 1, Release 16

V-12049

Added the "nettl" network analysis tool to the requirement.

IBM DB2 V10.5 LUW STIG, Version 1, Release 2

V-74501

Added not-a-finding statement to Check.

IIS 7.0 Site STIG, Version 1, Release 16

V-2240

Fix text "appcmd set config /section:system.applicationHost/sites "/[name='SITENAME'].limits. maxConnections:X" /commit:apphost" should be:

"appcmd.exe set config -section:system.applicationHost/sites "/[name='Default Web Site'].limits.maxConnections:X" /commit:apphost"

V-26026

Setting should be SHA256 instead of SHA2.

IIS 8.5 Server STIG, Version 1, Release 2

V-76691

Modified check criteria to be in sync with IISW-SI-000212.

V-76723

Modified to provide alternative method for meeting the requirement.

V-76725

Modified to provide alternative method for meeting the requirement.

V-76727

Modified to provide alternative method for meeting the requirement.

IIS 8.5 Site STIG, Version 1, Release 2

V-76777

Modified to provide alternative method for meeting the requirement.

V-76793

Modified check criteria to be in sync with IISW-SV-000113.

V-76841

Modified check criteria for additional acceptable values.

V-76869

Modified to provide alternative method for meeting the requirement.

Infoblox 7.x DNS STIG, Version 1, Release 5

V-68633

Add exceptions to Check/Fix regarding CNAME records. Also expound in Vulnerability Discussion.

Infrastructure L3 Switch STIG - Cisco, Version 8, Release 25

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Infrastructure L3 Switch STIG, Version 8, Release 25

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Infrastructure Router STIG - Cisco, Version 8, Release 25

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Infrastructure Router STIG - Juniper, Version 8, Release 25

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Infrastructure Router STIG, Version 8, Release 25

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

IPSec VPN Gateway STIG, Version 1, Release 14

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Juniper SRX SG ALG STIG, Version 1, Release 2

V-66333

Update the Check and Fix text to match the policy requirement.

Layer 2 Switch STIG - Cisco, Version 8, Release 23

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Layer 2 Switch STIG, Version 8, Release 23

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

McAfee Application Control 7.x STIG, Version 1, Release 3

V-74245

Removed check as requirement was accounted for in V-74243.

McAfee VirusScan 8.8 Local Client STIG, Version 5, Release 14

V-42571

Modified registry key for correct allowed value(s).

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

V-6585

Modified check criteria to allow for alternative method for validation.

V-6599

Modified check criteria to allow for alternative method for validation.

V-6600

Modified check criteria to allow for alternative method for validation.

V-6601

Modified check criteria to allow for alternative method for validation.

V-6602

Modified check criteria to allow for alternative method for validation.

V-6604

Modified check criteria to allow for alternative method for validation.

V-6611

Modified check criteria to allow for alternative method for validation.

V-6612

Modified check criteria to allow for alternative method for validation.

V-6614

Modified check criteria to allow for alternative method for validation.

V-6615

Modified check criteria to allow for alternative method for validation.

V-6616

Modified check criteria to allow for alternative method for validation.

V-6617

Modified check criteria to allow for alternative method for validation.

V-6618

Modified check criteria to allow for alternative method for validation.

V-6620

Modified check criteria to allow for alternative method for validation.

V-6625

Modified check criteria to allow for alternative method for validation.

V-6627

Modified check criteria to allow for alternative method for validation.

V-14654

Modified check criteria to allow for alternative method for validation.

V-42532

Modified check criteria to allow for alternative method for validation.

V-42533

Modified check criteria to allow for alternative method for validation.

V-42534

Modified check criteria to allow for alternative method for validation.

V-42538

Modified registry key for correct allowed value(s).

Microsoft Internet Explorer 11 Benchmark, Version 1, Release 11

Benchmark Update

Repackaged benchmark to accommodate manual STIG updates.

Microsoft Internet Explorer 11 STIG, Version 1, Release 14

V-46629

Downgrade to CAT III.

Microsoft Publisher 2016 Benchmark, Version 1, Release 2

V-70763

Corrected OVAL registry_state value datatype to facilitate content validation.

Microsoft SQL Server 2012 Database STIG, Version 1, Release 16

V-40911

Added not-a-finding statement to Check.

Microsoft SQL Server 2012 Instance STIG, Version 1, Release 16

V-41202

Removed CONNECT SQL from the requirement.

Microsoft SQL Server 2012 STIG, Version 1, Release 16

V-41036

Reworded Discussion to acknowledge possibility of conflict with other requirements.

V-41047

Updated CCI.

V-41389

Discussion and Fix reworded to accommodate the unavailability of codeplex.com.

V-41391

Discussion and Fix reworded to accommodate the unavailability of codeplex.com.

V-41392

Discussion and Fix reworded to accommodate the unavailability of codeplex.com.

Documentation Update

Supplemental Procedures - Added disclaimer.

Microsoft SQL Server 2014 Database STIG, Version 1, Release 6

V-67377

Restored to STIG - deleted by mistake.

V-67401

Discussion and Fix reworded to accommodate the unavailability of codeplex.com.

V-67403

Discussion and Fix reworded to accommodate the unavailability of codeplex.com.

V-67405

Discussion and Fix reworded to accommodate the unavailability of codeplex.com.

V-67877

Added not-a-finding statement to Check.

Documentation Update

Supplemental Procedures - Added disclaimer.

Microsoft SQL Server 2014 Instance STIG, Version 1, Release 7

V-67787

Corrected missing NOT making Check wrong.

Documentation Update

Supplemental Procedures - Added disclaimer.
Supplemental Procedure - Audit.sql - Added notes on alternative techniques.

Microsoft Windows 2012 Server DNS STIG, Version 1, Release 8

V-58547

Modified check finding statement to reference Windows 2012 instead of Windows 2008.

V-58551

Modified check criteria to identify required data elements to audit.

V-58555

Modified check criteria to identify required data elements to audit.

V-58587

Added note with respect to AD-integrated zones.

Microsoft Windows Defender Antivirus STIG, Version 1, Release 3

V-75207

Updated Fix Text to remove erroneous "Advanced MAP" from the template path name.

Mozilla Firefox STIG, Version 4, Release 21

V-15986

Remove window flip/sizing portion of check/fix as they are handled in other checks.

V-79053

Add new check similar to disabling crash reporting in Internet Explorer (V-46811). There should be no background submission of technical and other information from DoD computers to Mozilla with portions posted publically. Ensure the preferences in mozilla.cfg for "datareporting.healthreport.service.enabled" is set to "false" and locked.

Multifunction Device and Network Printers STIG, Version 2, Release 11

V-6794

Added Apple AirPrint to the check as not being allowed to send print jobs directly to a printer or MFD. Removed Responsibility.

Network Device Management SRG, Version 2, Release 13

V-55037

Modify SRG-APP-000023-NDM-000205 (V-55037) to remove references to SV-69283r3.

V-55105

Modify SRG-APP-000149-NDM-000247 (V- 55105) to remove references to CAC and clarify MFA implementation.

V-55119

Modify SRG-APP-000166-NDM-000254 (V-55119) to clarify conditions for password use.

V-55121

Modify SRG-APP-000167-NDM-000255 (V-55121) to clarify conditions for password use.

V-55123

Modify SRG-APP-000168-NDM-000256 (V-55123) to clarify conditions for password use.

V-55125

Modify SRG-APP-000169-NDM-000257 (V-55125) to clarify conditions for password use.

V-55127

Modify SRG-APP-000170-NDM-000329 (V-55127) to clarify conditions for password use.

V-55131

Update vulnerability discusstion "encrypted representations of passwords" to add information about password hashing. Add that hashing is the preferred mechanism while encrypted passwords are allowed for use cases where protections are used to ensure keys are protected. Also add that clear text passwords are not retained in any way after the auth process completes.

V-55157

Modify SRG-APP-000109-NDM-000233 (V- 55157) to clarify availability as an overriding concern.

V-55295

Modify SRG-APP-000516-NDM-000334 (V-55295) to include control AU-12a and CCI-000169.

Network Devices STIG, Version 8, Release 21

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

V-17840

Changed CHAP to EAP. Removed Responsibility.

Network Infrastructure Policy STIG, Version 9, Release 5

V-66397

Updated Check Content section to include missing word "not".

Network SRG, Version 2, Release 0-7

V-27301

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-27345

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-27450

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-27454

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-27495

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-27497

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45051

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-45053

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-45289

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45417

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45421

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45423

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-45559

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

Operating System SRG, Version 2, Release 0-6

V-44295

SRG Templates remove "Requires further clarification from NIST." from requirement and vulnerability discussion.

V-44305

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-44357

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-44405

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-44407

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

V-44409

Update the requirement and vulnerability discussion to remove SSL references and match current DoD encryption requirement.

Oracle Database 11.2g STIG, Version 1, Release 13

V-52141

Made it OK not to set archive mode when databases used solely for ETL are concerned.

V-52143

Added not-a-finding statement to Check.

V-52291

Modified Discussion, Check, and Fix with respect to PASSWORD_GRACE_TIME.

V-52293

Added a not-a-finding statement to Check.

V-52327

Better Check, to avoid false negatives.

V-52333

CCI updated.

V-52411

Deleted. Requirement has been removed from SRG.
Replaced DBA_USERS with SYS.USER$ in Check.

V-52413

Deleted. Requirement has been removed from SRG.

V-54055

Clarified "Remote Administration".

V-57615

Changed not a finding to not applicable (NA). Removed TRUE from list of acceptable values.

Documentation Update

Supplemental Procedures - Corrected dead references.

Oracle Database 12c STIG, Version 1, Release 9

V-61415

Modified Check to accommodate changes in 12c.

V-61439

Removed a dead reference to O121-BP-021800.

V-61523

Clarified "Remote Administration".

V-61539

Better Check, to avoid false negatives.

V-61545

CCI updated.

V-61571

Changed CHANGE PASSWORD to ALTER USER.

V-61645

Redundant, superseded Rule removed.

V-61739

Modified Discussion, Check, and Fix with respect to PASSWORD_GRACE_TIME.

V-61741
Added a not-a-finding statement to Check.

V-61759
Redundant, superseded Rule removed.

V-61769
Made it OK not to set archive mode when databases used solely for ETL are concerned.

V-61771
Added not-a-finding statement to Check.

V-61861
Deleted. Requirement has been removed from SRG.
Replaced DBA_USERS with SYS.USER$ in Check.

V-61863
Deleted. Requirement has been removed from SRG.

V-61965
Changed not a finding to not applicable (NA).

Documentation Update
Supplemental Procedures - Corrected dead references.

Oracle JRE 8 Windows STIG, Version 1, Release 5

V-66947
Add note stating if JWS is not enabled then the check is NA.

Oracle WebLogic Server 12c STIG, Version 1, Release 4

V-56299
Update check and the fix: By default, the following message should be displayed in the logs for Oracle WebLogic 12c; "Changing the default Random Number Generator in RSA CryptoJ from ECDRBG128 to HMACDRBG." For a complete list of FIPS 140-2-validated modules that are employed by WebLogic (RSA CryptoJ), please reference the NIST Crypto Module Validation Program web site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057

V-56301

Update check and the fix: By default, the following message should be displayed in the logs for Oracle WebLogic 12c; "Changing the default Random Number Generator in RSA CryptoJ from ECDRBG128 to HMACDRBG." For a complete list of FIPS 140-2-validated modules that are employed by WebLogic (RSA CryptoJ), please reference the NIST Crypto Module Validation Program web site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057

V-56313

Update check and the fix: By default, the following message should be displayed in the logs for Oracle WebLogic 12c; "Changing the default Random Number Generator in RSA CryptoJ from ECDRBG128 to HMACDRBG." For a complete list of FIPS 140-2-validated modules that are employed by WebLogic (RSA CryptoJ), please reference the NIST Crypto Module Validation Program web site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057

Perimeter L3 Switch STIG - Cisco, Version 8, Release 28

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Perimeter L3 Switch STIG, Version 8, Release 28

V-14671

Added exception to allowing downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Perimeter Router STIG - Cisco, Version 8, Release 28

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Perimeter Router STIG - Juniper, Version 8, Release 28

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

Perimeter Router STIG, Version 8, Release 28

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

PostgreSQL 9.x STIG, Version 1, Release 2

V-72841

Removed directive sudo su - postgres before postgres service restart (compare to V-72843);
Changed $ systemctl restart postgresql-9.5 TO $ sudo systemctl restart postgresql-9.5;
Changed $ service postgresql-9.5 restart TO $ sudo service postgresql-9.5 restart;
Replaced all occurrences of 9.5 with ${PGVER?}.

V-72843

Changed postgres restart to reload; replaced all occurrences of 9.5 with ${PGVER?}.

V-72847

Corrected missing apostrophe.

V-72851

Removed directive sudo su - postgres before postgres service reload (compare to V-72843);
Changed $ systemctl restart postgresql-9.5 TO $ sudo systemctl restart postgresql-9.5;
Changed $ service postgresql-9.5 restart TO $ sudo service postgresql-9.5 restart;
Replaced all occurrences of 9.5 with ${PGVER?}.

V-72853

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72859

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72863

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72885

Corrected missing apostrophe.

V-72887

Change postgres restart to reload.
Replaced all occurrences of 9.5 with ${PGVER?}.

V-72889

Changed
$ grep "client_min_messages"
${PGDATA?}/postgresql.conf
To single line $ grep "client_min_messages" ${PGDATA?}/postgresql.conf

Corrected missing apostrophe.

V-72897

Added missing closing " to $ psql -c "CREATE SCHEMA test AUTHORIZATION bob.

V-72901

Changed "of the PostgreSQL " to "of the PostgreSQL software library".

V-72905

Remove trailing semi-colon in OR NOT proconfig IS NULL;" and SECURITY INVOKER;".

V-72907

Reconcile syntax CREAT in command with CRT in log lines; replaced all occurrences of 9.5 with ${PGVER?}.

V-72909

Change $ vi 'log_destination' ${PGDATA?}/postgresql.conf to $ vi ${PGDATA?}/postgresql.conf; replaced all occurrences of 9.5 with ${PGVER?}.

V-72915

Corrected missing apostrophes; replaced all occurrences of 9.5 with ${PGVER?}.

V-72919

Remove `pgaudit` tick marks; replaced all occurrences of 9.5 with ${PGVER?}.

V-72923

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72925

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72929

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72931

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72933

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72939

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72945

Add trailing semi-colon to ALTER ROLE joe NOLOGIN" as in ALTER ROLE joe NOLOGIN;";.

Change log line output from drop role/DROP ROLE to alter role/ALTER ROLE to match SQL command.

V-72947

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72949

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72953

Fixed spacing and replaced semi-colons with commas or periods in:
TRUNCATE TABLE;DELETE, or DELETE affecting more than n rows, for some n, or DELETE without a WHERE clause;
UPDATE or UPDATE affecting more than n rows, for some n, or UPDATE without a WHERE clause;
Replaced all occurrences of 9.5 with ${PGVER?}.

V-72955

Removed `pgaudit` tick marks;
Removed dollar sign from $9.5 in $ sudo systemctl reload postgresql-$9.5;
Replaced all occurrences of 9.5 with ${PGVER?}.

V-72957

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72959

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72961

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72963

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72965

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72971

Removed `pgaudit` 3x, `role`, `read`, `write`, and `ddl`, `on` tick marks; replaced all occurrences of 9.5 with ${PGVER?}.

V-72973

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72975

Add trailing semi-colon to $ psql -c "SET ROLE bob; REVOKE ALL PRIVILEGES ON test FROM bob".

V-72977

Add trailing semi-colon to $ psql -c "CREATE ROLE bob; CREATE TABLE test(id INT)".

V-72979

Change $ grep hostssl ${PGDATA?}/postgresql.conf to $ grep hostssl ${PGDATA?}/pg_hba.conf; replaced all occurrences of 9.5 with ${PGVER?}.

V-72981

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72985

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72987

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72991

Replaced all occurrences of 9.5 with ${PGVER?}.

V-72995

Added not-a-finding statement to Check.

V-73001

Change $ psql -c "SHOW logging_destination" to $ psql -c "SHOW log_destination".

V-73005

Removed quotes around "log_hostname"; replaced all occurrences of 9.5 with ${PGVER?}.

V-73007

Changed PostgreSQLs to PostgreSQL; changed $ psql -c "select * from pg_extension where extname != 'plpgsql';"" TO $ psql -c "select * from pg_extension where extname != 'plpgsql'".

V-73011

Changed PostgreSQLs to PostgreSQL.

V-73015

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73017

Change $ psql -c "REVOKE ALL PRIVILEGES ON <table> FROM <role_name>; TO $ psql -c "REVOKE ALL PRIVILEGES ON <table> FROM <role_name>"

V-73019

Remove single quote in Next, review the current shared_preload_libraries'; replaced all occurrences of 9.5 with ${PGVER?}.

V-73021

Removed trailing semi-colon from:
pgaudit.log = 'write, ddl, role, read, function';
pgaudit.log_relation = on;
Removed function from pgaudit.log = 'write, ddl, role, read, function' OR add to If pgaudit.log does not contain ddl, role, read, write, this is a finding. (reconcile);
Replaced all occurrences of 9.5 with ${PGVER?}.

V-73023

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73025

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73029

Change $ sudo systemctl restartpostgresql-9.5 TO $ sudo systemctl restart postgresql-9.5; replaced all occurrences of 9.5 with ${PGVER?}.

V-73033

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73037

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73039

Removed trailing period after $ sudo chown -R root:root /usr/pgsql-9.5/share/contrib/pgaudit; replaced all occurrences of 9.5 with ${PGVER?}.

V-73041

Added closing) to As the database administrator (usually postgres, run the following SQL; replaced all occurrences of 9.5 with ${PGVER?}.

V-73043

Fixed $ sudo chown -R root:root /usr/pgsql-9.5/share/contrib/pgaudit MATCH the check for /usr/pgsql-9.5/bin|share|include ?; replaced all occurrences of 9.5 with ${PGVER?}.

V-73045

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73047

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73051

Changed WHERE username to usename in SELECT pg_terminate_backend(pid) FROM pg_stat_activity WHERE username='<username>';

V-73057

Changed PostgreSQLs to PostgreSQL.

V-73059

Changed PostgreSQLs to PostgreSQL.

V-73065

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73067

Reconcile/Verify that role, read, write, and ddl auditing are enabled: AND If the output does not contain read and write, this is a finding. -- pgaudit.log = 'read, write'; replaced all occurrences of 9.5 with ${PGVER?}.

V-73069

Replaced all occurrences of 9.5 with ${PGVER?}.

V-73071

Corrected product name in Check.
Replaced Postgres Plus Advanced Server with PostgreSQL.

Red Hat 6 Benchmark, Version 1, Release 18

V-38513

Disabled Rule in OVAL due to check procedure incompatibilities with OVAL.

Red Hat Enterprise Linux 6 STIG, Version 1, Release 18

V-38447

Updated the finding statement to focus on system binaries. Updated the "rpm" command in the fix to produce the correct output.

V-38513

Updated the check command to look at the current iptables running configuration.

V-38686

Updated the check command to look at the current iptables running configuration.

Red Hat Enterprise Linux 7 Benchmark, Version 1, Release 2

Benchmark Update

Repackaged benchmark to accommodate manual STIG updates.

Red Hat Enterprise Linux 7 STIG, Version 1, Release 4

V-71859

Removed the allowance for the use of the short banner. Added the "dconf update" command to the Fix.

V-71863

Removed the allowance for the use of the short banner.

V-71895

The configuration referenced does not exist.

V-71899

Updated the example output in the Check Content. Added the "dconf update" command to the Fix.

V-71901

Updated the finding statement to reflect an allowed maximum value. Added the "dconf update" command to the Fix.

V-71961

Added a finding statement that requires the "superusers-account" be set to root. Updated the Fix text to reflect the correct grub commands and file locations.

V-71963

Added a finding statement that requires the "superusers-account" be set to root. Updated the Fix text to reflect the correct grub commands and file locations.

V-71991

Updated typographical errors in the check content.

V-72007

Removed the "-xdev" option from the check command.

V-72009

Removed the "-xdev" option from the check command.

V-72019

Removed the note from the check about privileged UID's and revised the finding statement to be more specific to the requirement.

V-72021

Removed the note from the check about privileged UID's.

V-72067

Removed wording from the Fix that indicated "prelink" must be disabled.

V-72081

Updated the example output and finding statements to reference the correct variable.

V-72095

Corrected command in Fix instructions.

V-72097

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72099

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72101

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72103

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72105

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72107

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72109

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72111

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72113

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72115

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72117

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72119

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72121

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72123

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72125

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72127

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72129

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72131

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72133

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72151

Updated command path in Check and Fix instructions.

V-72159

Updated command path in Check and Fix instructions.

V-72171

Updated the "grep" command in the check and the example output in the Check and Fix content. Updated the finding statements. Added a note to the fix to explain the dual architectures listed.

V-72187

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72189

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72199

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72201

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72203

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72205

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72207

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the dual architectures listed.

V-72237

Updated the check command to use "clientaliveinterval". Updated the finding statements to reflect the acceptable range of values for the setting.

V-72241

Add note about the OS version as related to the relevant variable setting.

V-72251

Add note about the OS version as related to the relevant variable setting.

V-72291

Updated command path in Check and Fix instructions.

V-72299

Updated the requirement to look for the vsftpd package instead of the lftpd package.

V-72303

Updated typographical errors in the check and fix content.

V-72427

Updated configuration file path in Check and Fix.

V-72433

Updated Check instructions regarding PAM configuration.

V-72435

Removed RHEL-07-041004 as RHEL-07-010500 covers all users.

V-73155

Updated the Rule Title to reference the GUI.

V-73157

Updated the Rule Title to reference the GUI.

V-73159

Updated the "grep" command and the finding statement in the check. Added a note to the fix to explain the acceptable range of values.

V-78995

Added a requirement to configure the /org/gnome/desktop/screensaver/lock-enabled setting.

V-78997

Added a requirement to configure the /org/gnome/desktop/screensaver/idle-activation-enabled setting.

V-78999

Added a new requirement to audit the "create_module" command.

V-79001

Added a new requirement to audit the "finit_module" command.

Solaris 10 SPARC Benchmark, Version 1, Release 20

Benchmark Update

Repackaged benchmark to accommodate manual STIG updates.

Solaris 10 SPARC STIG, Version 1, Release 21

V-22429

Updated IA control.

Solaris 10 X86 Benchmark, Version 1, Release 20

Benchmark Update

Repackaged benchmark to accommodate manual STIG updates.

Solaris 10 X86 STIG, Version 1, Release 21

V-22429

Updated IA control.

Voice Video Endpoint SRG, Version 1, Release 7

V-66701

Modify SRG-NET-000520-VVEP-00010 (V-66701) to include VRF implementations.

V-66703

Modify SRG-NET-000520-VVEP-00011 (V-66703) to include VRF implementations.

V-66705

Modify SRG-NET-000057-VVEP-00012 (V-66705) to include VRF implementations.

V-66719

Modify SRG-NET-000041-VVEP-00020 (V-66719) to remove references to DD Form 2056.

V-66725

Modify SRG-NET-000042-VVEP-00021 (V-66725) to remove references to DD Form 2056.

V-79055

Add SRG-NET-000041-VVEP-00064 (V-xxxxx) to place DD Form 2056 on unclassified hardware endpoints.

Voice Video Services Policy STIG, Version 3, Release 12

V-79051

Add VVT/VTC 1906 (V-xxxxx) to silence Voice Video endpoints with speakers.

Voice Video Session Management SRG, Version 1, Release 5

V-62149

Modify SRG-NET-000520-VVSM-00024 (V-62149) to include VRF implementations.

V-62151

Modify SRG-NET-000520-VVSM-00025 (V-62151) to include VRF implementations.

Windows 10 Benchmark, Version 1, Release 10

V-63377

Modified benchmark tests to verify the status of the IIS features using wmi57 tests in lieu of registry tests.

V-70639

Updated OVAL content for the SMBv1 Protocol requirement to be used by the Windows Server 2016 benchmark.

V-74719

Updated the OVAL content for the "Secondary Logon" service test comment to accurately reference the "Secondary Logon" service and not the "Smart Card Removal Policy" service.

V-74723

Updated OVAL content for the SMBv1 Server requirement to be used by the Windows Server 2016 benchmark.

V-74725

Updated OVAL content for the SMBv1 Client requirement to be used by the Windows Server 2016 benchmark.

Windows 10 STIG, Version 1, Release 12

V-63845

Updated to note allowed exception to Access this computer from the network user right.

V-78129

Added requirement that administrator accounts must not be used for Internet access, consistent with other Windows STIGs.

Documentation Update

Updated query in Windows Apps section of STIG Overview.

Windows 2008 DC Benchmark, Version 6, Release 41

Benchmark Update

Repackaged benchmark to accommodate manual STIG update.

Windows 2008 DC STIG, Version 6, Release 39

V-15823

Clarified noted exceptions.

Windows 2008 MS Benchmark, Version 6, Release 41

Benchmark Update

Repackaged benchmark to accommodate manual STIG update.

Windows 2008 MS STIG, Version 6, Release 39

V-15823

Clarified noted exceptions.

Windows 2008 R2 DC Benchmark, Version 1, Release 27

V-26532

Removed OVAL content from the benchmark as the requirement has been removed from the manual STIG.

V-26554

Removed OVAL content from the benchmark as the Audit Security State Change (Failure) requirement has been removed from the manual STIG.

V-57633

Added new OVAL content for the Audit Authorization Policy Change (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78057

Added new OVAL content for the Audit Account Lockout (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78059

Added new OVAL content for the Audit Account Lockout (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78061

Added new OVAL content for the Audit Other System Events (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78063

Added new OVAL content for the Audit Other System Events (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

Windows 2008 R2 DC STIG, Version 1, Release 25

V-15823

Clarified noted exceptions.

V-26531

Updated Audit Computer Account Management Success requirement to apply to Domain Controllers only.

V-26532

Removed Audit Computer Account Management Failures to align with Windows 2016 STIG.

V-26554

Removed Audit Security State Change Failures to align with Windows 2016 STIG.

V-57633

Added Audit Authorization Policy Change Successes to align with Windows 2016 STIG.

V-78057

Added Audit Account Lockout Successes to align with Windows 2016 STIG.

V-78059

Added Audit Account Lockout Failures to align with Windows 2016 STIG.

V-78061

Added Audit Other System Events Successes to align with Windows 2016 STIG.

V-78063

Added Audit Other System Events Failures to align with Windows 2016 STIG.

Windows 2008 R2 MS Benchmark, Version 1, Release 28

V-26531

Removed OVAL content from the benchmark as the requirement has been removed from the manual member server STIG.

V-26532

Removed OVAL content from the benchmark as the requirement has been removed from the manual STIG.

V-26554

Removed OVAL content from the benchmark as the Audit Security State Change (Failure) requirement has been removed from the manual STIG.

V-57633

Added new OVAL content for the Audit Authorization Policy Change (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78057

Added new OVAL content for the Audit Account Lockout (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78059

Added new OVAL content for the Audit Account Lockout (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78061

Added new OVAL content for the Audit Other System Events (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78063

Added new OVAL content for the Audit Other System Events (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

Windows 2008 R2 MS STIG, Version 1, Release 25

V-15823

Clarified noted exceptions.

V-26531

Updated Audit Computer Account Management Success requirement to apply to Domain Controllers only.

V-26532

Removed Audit Computer Account Management Failures to align with Windows 2016 STIG.

V-26554

Removed Audit Security State Change Failures to align with Windows 2016 STIG.

V-57633

Added Audit Authorization Policy Change Successes to align with Windows 2016 STIG.

V-78057

Added Audit Account Lockout Successes to align with Windows 2016 STIG.

V-78059

Added Audit Account Lockout Failures to align with Windows 2016 STIG.

V-78061

Added Audit Other System Events Successes to align with Windows 2016 STIG.

V-78063

Added Audit Other System Events Failures to align with Windows 2016 STIG.

Windows 2012/2012 R2 DC Benchmark, Version 2, Release 11

V-26532

Removed OVAL content from the benchmark as the requirement has been removed from the manual STIG.

V-26554

Removed OVAL content from the benchmark as the Audit Security State Change (Failure) requirement has been removed from the manual STIG.

V-36707

Updated the OVAL content for the SmartScreen requirement to be a finding if SmartScreen is not enabled in conjunction with the change to the manual STIG.

V-57633

Updated OVAL content for the Audit Authorization Policy Change (Success) requirement to be used by the Windows Server 2012 R2 benchmarks.

V-57635

Removed OVAL content from the benchmark as the requirement has been removed from the manual STIG.

V-78057

Added new OVAL content for the Audit Account Lockout (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78059

Added new OVAL content for the Audit Account Lockout (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78061

Added new OVAL content for the Audit Other System Events (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78063

Added new OVAL content for the Audit Other System Events (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

Windows 2012/2012 R2 DC STIG, Version 2, Release 11

V-6840

Updated to use Windows queries instead of DumpSec application.

V-7002

Updated to use Windows queries instead of DumpSec application.

V-14225

Updated to use Windows queries instead of DumpSec application.

V-15823

Clarified noted exceptions.

V-26531

Updated Audit Computer Account Management Success requirement to apply to Domain Controllers only.

V-26532

Removed Audit Computer Account Management Failures to align with Windows 2016 STIG.

V-26554

Removed Audit Security State Change Failures to align with Windows 2016 STIG.

V-36662

Updated to use Windows queries instead of DumpSec application.

V-36707

Changed SmartScreen requirement to align with other Windows STIGs - Enabled and CAT II.

V-57635

Removed Audit Authorization Policy Change Failures to align with Windows 2016 STIG.

V-78057

Added Audit Account Lockout Successes to align with Windows 2016 STIG.

V-78059

Added Audit Account Lockout Failures to align with Windows 2016 STIG.

V-78061

Added Audit Other System Events Successes to align with Windows 2016 STIG.

V-78063

Added Audit Other System Events Failures to align with Windows 2016 STIG.

Windows 2012/2012 R2 MS Benchmark, Version 2, Release 11

V-26531

Removed OVAL content from the benchmark as the requirement has been removed from the manual member server STIG.

V-26532

Removed OVAL content from the benchmark as the requirement has been removed from the manual STIG.

V-26554

Removed OVAL content from the benchmark as the Audit Security State Change (Failure) requirement has been removed from the manual STIG.

V-36707

Updated the OVAL content for the SmartScreen requirement to be a finding if SmartScreen is not enabled in conjunction with the change to the manual STIG.

V-57633

Updated OVAL content for the Audit Authorization Policy Change (Success) requirement to be used by the Windows Server 2012 R2 benchmarks.

V-57635

Removed OVAL content from the benchmark as the requirement has been removed from the manual STIG.

V-78057

Added new OVAL content for the Audit Account Lockout (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78059

Added new OVAL content for the Audit Account Lockout (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78061

Added new OVAL content for the Audit Other System Events (Success) requirement in conjunction with the addition of the requirement to the manual STIG.

V-78063

Added new OVAL content for the Audit Other System Events (Failure) requirement in conjunction with the addition of the requirement to the manual STIG.

Windows 2012/2012 R2 MS STIG, Version 2, Release 11

V-6840

Updated to use Windows queries instead of DumpSec application.

V-7002

Updated to use Windows queries instead of DumpSec application.

V-14225

Updated to use Windows queries instead of DumpSec application.

V-15823

Clarified noted exceptions.

V-26531

Updated Audit Computer Account Management Success requirement to apply to Domain Controllers only.

V-26532

Removed Audit Computer Account Management Failures to align with Windows 2016 STIG.

V-26554

Removed Audit Security State Change Failures to align with Windows 2016 STIG.

V-36662

Updated to use Windows queries instead of DumpSec application.

V-36707

Changed SmartScreen requirement to align with other Windows STIGs - Enabled and CAT II.

V-57635

Removed Audit Authorization Policy Change Failures to align with Windows 2016 STIG.

V-78057

Added Audit Account Lockout Successes to align with Windows 2016 STIG.

V-78059

Added Audit Account Lockout Failures to align with Windows 2016 STIG.

V-78061

Added Audit Other System Events Successes to align with Windows 2016 STIG.

V-78063

Added Audit Other System Events Failures to align with Windows 2016 STIG.

Windows 2016 STIG, Version 1, Release 3

V-73241

Removed specific antivirus product referenced.

V-73259

Corrected note referring to built-in administrator as disabled instead of renamed.

V-73299

Updated to allow alternate method for disabling SMBv1.

V-73375

Clarified changes from schema update to support Exchange are not a finding.

V-73431

Corrected STIG ID referenced in check.

V-73443

Corrected STIG ID referenced in check.

V-73445

Corrected STIG ID referenced in check.

V-73447

Corrected STIG ID referenced in check.

V-73477

Corrected STIG ID referenced in check.

V-73479

Corrected STIG ID referenced in check.

V-73535

Removed untrusted font blocking requirement due to issues.

V-73605

Clarified details apply to unclassified systems, refers to PKE documentation for other systems.

V-73615

Clarified various formats may exist for individual identifiers.

V-73647

Removed short version of banner text as NA.

V-78123

Added as alternate method for disabling SMBv1 server.

V-78125

Added as alternate method for disabling SMBv1 client.

V-78127

Added requirement for unresolved SIDs found on user rights.

Windows 7 Benchmark, Version 1, Release 35

V-3347

Modified benchmark tests to verify the status of the IIS features using wmi57 tests in lieu of registry tests.

V-68843

Making sure a change made during the Windows 10 1709 OOCR to keep the Windows 7 content checking for the right value gets propagated.

V-68847

Making sure a change made during the Windows 10 1709 OOCR to keep the Windows 7 content checking for the right value gets propagated.

Windows 7 STIG, Version 1, Release 29

V-26470

Updated to note allowed exception to Access this computer from the network user right.

Windows 8/8.1 Benchmark, Version 1, Release 21

V-3347

Modified benchmark tests to verify the status of the IIS features using wmi57 tests in lieu of registry tests.

Windows 8/8.1 STIG, Version 1, Release 20

V-26470

Updated to note allowed exception to Access this computer from the network user right.

V-73519

Corrected reference to Windows 10.

V-73523

Corrected reference to Windows 10.

Windows Server 2016 Benchmark, Version 1, Release 4

V-73299

Added new OVAL content for the SMBv1 Protocol requirement.

V-73405

New OVAL development for Windows Server 2016.

V-73407

New OVAL development for Windows Server 2016.

V-73409

New OVAL development for Windows Server 2016.

V-73495

Updated platform-specification for applicability determinations.

V-73509

Updated platform-specification for applicability determinations.

V-73533

Updated platform-specification for applicability determinations.

V-73651

Updated platform-specification for applicability determinations.

V-78123

Added new OVAL content for the SMBv1 Server requirement.

V-78125

Added new OVAL content for the SMBv1 Client requirement.

Benchmark Update

Updated platform-specification for applicability determinations.

WLAN Access Point (Enclave-NIPRNet Connected) STIG, Version 6, Release

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

WLAN Access Point (Internet Gateway Only Connection) STIG, Version 6, Re

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

WLAN Bridge STIG, Version 6, Release 13

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

WLAN Controller STIG , Version 6, Release 13

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

WMAN Access Point STIG , Version 6, Release 12

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

WMAN Bridge STIG, Version 6, Release 12

V-14671

Added exception to allow downgrading to a CAT III if using MD5 for NTP authentication. Removed reference to PKI.

z/OS ACF2 STIG, Version 6, Release 34

V-119

Allow Specific System Programmer Level batch job Alter access to Master Catalog.

V-7050

Remove Unique ID REQMNT from ZUSS0048.

V-65647

Clarification of ACF0395.

Documentation Update

Correct Typo in Table 7.1: Controls on z/OS System Commands.

z/OS Automated PDI list spreadsheet, Version 6, Release 34

Documentation Update

Added automation of System Programming commands (SPI).

New

New requirement for AES Encryption for CA-TSS.

z/OS Cross Ref of SRRAUDIT spreadsheet, Version 6, Release 34

Documentation Update

Added automation of System Programming commands (SPI).

Changes to add new resources for analysis under z/OS 2.3.

z/OS IBM CICS Transaction Server for ACF2, Version 6, Release 4

V-17982

Update ZCIC0021 with automation content.

z/OS IBM CICS Transaction Server for RACF, Version 6, Release 4

V-17982

Update ZCIC0021 with automation content.

z/OS IBM CICS Transaction Server for TSS, Version 6, Release 4

V-17982

Update ZCIC0021 with automation content.

z/OS IBM SDSF for ACF2, Version 6, Release 9

Documentation Update

Update Table 11.28: SDSF Server OPERCMDS Resources.

z/OS IBM SDSF for RACF, Version 6, Release 9

Documentation Update

Update Table 11.28: SDSF Server OPERCMDS Resources.

z/OS IBM SDSF for TSS, Version 6, Release 9

Documentation Update

Update Table 11.28: SDSF Server OPERCMDS Resources.

z/OS PDI list spreadsheet, Version 6, Release 34

Documentation Update

Added automation of System Programming commands (SPI).

New

New requirement for AES Encryption for CA-TSS.

z/OS RACF STIG, Version 6, Release 34

V-119

Allow Specific System Programmer Level batch job Alter access to Master Catalog.

V-7050

Remove Unique ID REQMNT from ZUSS0048.

Documentation Update

Correct Typo in Table 7.1: Controls on z/OS System Commands.

z/OS SRR Scripts, Version 6, Release 34

New

New requirement for AES Encryption for CA-TSS.

SRR Script Update

Added automation of System Programming commands (SPI).

Changes to add new resources for analysis under z/OS 2.3.

Correct issue with analysis of SMF subtype records.

Change to remove RACF STC from STCILIST member to prevent SYS1.BRODCAST from being analyzed.

Change WRNDAYS to 1-10 range.

Corrected issue where all users have access in permissions and requirements specify that all users are not to have access, only authorized users are allowed access.

Change e-mail address specified for issues with scripts.

Change field in xml dataset from OS390 to z/OS.

Change to remove ZFS STC from STCILIST member to prevent evaluation of unnecessary datasets.

Corrected issue with evaluation of ACF2 resources when resource is not defined to ACF2.

z/OS TSS STIG, Version 6, Release 34

V-119

Allow Specific System Programmer Level batch job Alter access to Master Catalog.

V-7050

Remove Unique ID REQMNT from ZUSS0048.

V-79049

New requirement for AES Encryption for CA-TSS.

Documentation Update

Correct Typo in Table 7.1: Controls on z/OS System Commands.