

October 2016 STIGs to be Released

Release Date: October 28, 2016

Adobe ColdFusion 11 STIG, Version 1, Release 2

V-62499

Modified to allow requirement setting to be set to 5 seconds (Match Request Timeout) or to a admin specified value that does not impact application function.

V-62507

Modified to allow requirement setting to be set to set to 50 or as low as the hosted applications allow.

AIX 6.1 Benchmark, Version 1, Release 9

V-22310

Updated the OVAL to match the updated STIG requirement.

AIX 6.1 STIG, Version 1, Release 9

V-776

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-907

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11985

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11986

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-12765

Updated number of days allowed and file names in Check Content.

V-22354

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22355

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22359

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22360

October 2016 STIGs to be Released

Release Date: October 28, 2016

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22363

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22364

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

Apache 2.2 Server for Windows STIG, Version 1, Release 9

V-13724

Added clarification for instances where the settings is not explicitly set.

V-13725

Added clarification for instances where the settings is not explicitly set.

V-13726

Added clarification for instances where the settings is not explicitly set.

Apache 2.2 Site for Windows STIG, Version 1, Release 9

V-2240

Added clarification for instances where the settings is not explicitly set.

Apple OS X 10.11 STIG, Version 1, Release 2

V-67617

Updated AllowIdentifiedDevelopers in the Check Content to use the value of 1 instead of 0.

V-67673

Updated Check Content to permit emergency maintenance account that is present in the OS.

BlackBerry BES 12.5.x MDM STIG, Version 1, Release 2

Documentation Update

Updated all STIG documents to change BES 12.3.x to 12.5.x. Changed scope in Overview to include BES 12.3 through 12.5.

BlackBerry BES 5.x MDM STIG, Version 2, Release 9

V-19226

Minor updates to the Rule Title, Vulnerability Discussion, and Check. No change to the requirement.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Documentation Update

Split BES and BB OS STIGs into separate STIG packages.

Moved Configuration Tables document from BES STIG package to BB OS STIG package.

Updated all STIG documents with new release number and to conform with current style guide.

BlackBerry OS 10.3.x STIG, Version 1, Release 3

V-71491

Added new check for Hotspot Browser timeout to conform with current style guide..

V-71493

Added new check for Allow use of preloaded trusted root certificates.

Documentation Update

Added list of new IT Policy rules to the configuration table document, update release date, version number of all documents.

BlackBerry OS 7.x.x STIG, Version 2, Release 10

Documentation Update

Split BES and BB OS STIGs into separate STIG packages.

Moved Configuration Tables document from BES STIG package to BB OS STIG package.

Updated format of all documents to conform with current style guide.

Commercial Mobile Device (CMD) Policy STIG, Version 2, Release 5

V-24955

Updated Check Content to reflect current DoD policy.

V-24958

Updated Check Content.

V-24960

Updated Group Title clarify topic of check. Updated check procedure to clarify the procedure.

V-24961

Updated training requirements.

V-24962

Updated Check Content.

V-24963

October 2016 STIGs to be Released

Release Date: October 28, 2016

Updated Check Content to clarify requirement.

V-24965

Removed requirement as it is not handled via the AO app vetting process.

V-24966

Covered by the Network Infrastructure Policy STIG.

V-24968

Removed requirement as it is now covered by the MOS STIGs.

V-25034

Removed from the CMD Policy STIG as it is covered by the Network Infrastructure Policy STIG.

V-25035

Removed from the CMD Policy STIG as it is covered by the Network Infrastructure Policy STIG.

V-25036

Removed from the CMD Policy STIG as it is covered by the Network Infrastructure Policy STIG.

V-32674

Removed requirement as it is now covered by the MOS STIGs.

V-32677

Updated requirement to remove out-of-date procedures.

V-55941

Removed requirement as it is covered by WIR-SPP-021.

V-55943

Removed requirement as it is covered by WIR-SPP-021.

Documentation Update

Overview and history document minor updates.

Database SRG, Version 2, Release 5

V-32479

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-32555

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-32570

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-32571

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-58021

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-58179

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-58181

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-58183

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

DNS Policy STIG, Version 4, Release 1.20

V-13035

Modified Fix Text verbiage: WRT roles responsible for audit logs.

DoD Annex for the MDM Agent EP, Version 1, Release 2

Documentation Update

Updated based on changes to FPT_ITT.1, FAU_GEN.1.1(1), FAU_ALT_EXT.2.1. FAU_ALT_EXT.2.1 in the MDMPP DoD Annex.

DoD Annex for the MDMPP, Version 1, Release 3

Documentation Update

Updated entries for FPT_ITT.1, FAU_GEN.1.1(1), FAU_ALT_EXT.2.1. FAU_ALT_EXT.2.1.

DoD Annex to the cPP for Stateful Traffic Filter Firewalls 1.0, Version 1, Release 3

Documentation Update

October 2016 STIGs to be Released

Release Date: October 28, 2016

Changed SFRs to SFR Elements. Section 2-2 removed the words "Objective Functions" from the title and in first paragraph. changed the word objective to "optional and selection-based."

Moved mandated selections from Table 2.2 to Table 2.1.

EDB Postgres Advanced Server STIG, Version 1, Release 2

V-68955

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-68971

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-68973

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

V-68975

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-68977

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-68989

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-68991

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-69023

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

Exchange 2010 Mailbox Server STIG, Version 1, Release 8

V-33606

Reworded logging requirement to read "set to lowest at a minimum".

F5 BIG-IP Device Management 11.x STIG, Version 1, Release 3

V-60119

Removed requirement from the STIG. The application inherently meets the requirement.

October 2016 STIGs to be Released

Release Date: October 28, 2016

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

V-60281

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-60283

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-60285

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-60287

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-60289

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-60349

Corrected Check Content and Fix Text Sections.

Google Chrome STIG, Version 1, Release 6

V-44711

Added IA Control.

V-44713

Added IA Control.

V-44719

Added IA Control.

V-44723

Added IA Control.

V-44727

Added IA Control.

V-44729

Added IA Control.

Modified Step 3 of Check Content: "If the a registry value name of 1 does not exist under that key or its value is not set to....".

V-44733

Added IA Control.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-44735

Added IA Control.

V-44737

Added IA Control.

V-44739

Removed deprecated policy setting.

V-44741

Added IA Control.

V-44743

Added IA Control.

V-44745

Added IA Control.

V-44749

Added IA Control.

V-44751

Added IA Control.

V-44753

Added IA Control.

V-44757

Added IA Control.

V-44759

Added IA Control.

V-44761

Added IA Control.

V-44763

Added IA Control.

V-44765

Added IA Control.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-44769

Added IA Control.

V-44771

Added IA Control.

V-44773

Added IA Control.

V-44775

Added IA Control.

V-44777

Added IA Control.

V-44781

Added IA Control.

V-44783

Added IA Control.

V-44787

Added IA Control.

V-44789

Added IA Control.

V-44791

Added IA Control.

V-44793

Added IA Control.

V-44795

Added IA Control.

V-44799

Added IA Control.

Modified Check Content: "If this key both exists AND has any defined values, this is a finding."

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-44801

Removed Blank Home Page requirement.

V-44805

Added IA Control.

V-52795

Added IA Control.

HBSS ePO 5.x STIG, Version 1, Release 10

V-14499

Clarified paths in Check Content verbiage.

V-14506

Added clarification to requirement to move non-managed system rather than delete them.

V-14579

Bring check verbiage and fix verbiage in sync.

V-24175

Modified requirement to be NA if Agent Handlers are not being used.

V-24306

Removed "NOTE: See H50240 for labeling recommendation process." for clarity.

V-31133

Added clarification for backup as it pertains to ePO server keys.

HBSS HIP 8 STIG, Version 4, Release 17

V-14534

Added clarification for requirements for HIP user interface passwords.

V-60665

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

Updated requirement to replace signatures from 2297 to 7010 & 7035 per TO 14-0018.

V-60667

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

Updated requirement to replace signatures from 2297 to 7010 & 7035 per TO 14-0018.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-60669

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.
Modified signature references and reference to DTAM170.

V-71677

Added requirement for enabling and configuring signatures for SQL servers per TO 14-0018.

V-71679

Added requirement for enabling and configuring signatures for web server front end applications that have SQL server databases per TO 14-0018.

HBSS Remote Console STIG, Version 4, Release 13

V-24014

Added specifications for when and why user certificates should be removed after imported.

HPUX 11.31 Benchmark, Version 1, Release 13

V-22310

Updated the OVAL to match the updated STIG requirement.

V-22360

Updated the OVAL to match the updated STIG requirement.

V-22363

Updated the OVAL to match the updated STIG requirement.

V-22364

Updated the OVAL to match the updated STIG requirement.

HP-UX 11.31 STIG, Version 1, Release 12

V-776

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-907

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11985

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11986

October 2016 STIGs to be Released

Release Date: October 28, 2016

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-12765

Updated number of days allowed and file names in Check Content.

V-22354

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22355

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22359

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22360

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22363

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22364

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22496

Adjusted finding statement to be consistent with Rule Title.

IIS 7.0 Web Site STIG, Version 1, Release 11

V-2252

Modified check verbiage to not be in conflict with requirements of WG255 IIS7.

V-6724

Clarified check verbiage WRT IP address vs. FQDN.

V-13689

Modified check verbiage to not be in conflict with requirements of WG250 IIS7.

Joint Regional Security Stack ISCG, Version 1, Release 2

V-57829

October 2016 STIGs to be Released

Release Date: October 28, 2016

Removed requirement.

McAfee MOVE Agentless SVA STIG, Version 1, Release 5

V-43788

Made modifications as per comments from Program Office.

V-43957

Made modifications as per comments from Program Office.

V-43958

Made modifications as per comments from Program Office.

V-43959

Made modifications as per comments from Program Office.

V-43960

Made modifications as per comments from Program Office.

V-43961

Made modifications as per comments from Program Office.

V-43962

Made modifications as per comments from Program Office.

V-44931

Made modifications as per comments from Program Office.

V-44933

Made modifications as per comments from Program Office.

V-44935

Made modifications as per comments from Program Office.

V-44969

Made modifications as per comments from Program Office.

V-44973

Made modifications as per comments from Program Office.

V-44979

Made modifications as per comments from Program Office.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-44993

Made modifications as per comments from Program Office.

V-48853

Made modifications as per comments from Program Office.

V-48855

Made modifications as per comments from Program Office.

V-48857

Made modifications as per comments from Program Office.

V-48859

Made modifications as per comments from Program Office.

V-48861

Made modifications as per comments from Program Office.

V-48863

Made modifications as per comments from Program Office.

V-48865

Made modifications as per comments from Program Office.

V-48867

Made modifications as per comments from Program Office.

V-48869

Made modifications as per comments from Program Office.

V-48871

Made modifications as per comments from Program Office.

V-48873

Made modifications as per comments from Program Office.

Documentation Update

Made modifications as per comments from Program Office.

McAfee MOVE Multi-Platform Client STIG, Version 1, Release 5

V-42935

October 2016 STIGs to be Released

Release Date: October 28, 2016

Made modifications as per comments from Program Office.

V-42936

Made modifications as per comments from Program Office.

V-42937

Made modifications as per comments from Program Office.

V-42939

Made modifications as per comments from Program Office.

V-42940

Made modifications as per comments from Program Office.
Changed from 180 seconds to 45 seconds in Rule Title.

V-42942

Made modifications as per comments from Program Office.

V-42943

Made modifications as per comments from Program Office.

V-42944

Made modifications as per comments from Program Office.

V-42945

Made modifications as per comments from Program Office.

V-42946

Made modifications as per comments from Program Office.

V-42947

Made modifications as per comments from Program Office.

V-42948

Made modifications as per comments from Program Office.

V-42949

Made modifications as per comments from Program Office.

V-42950

Made modifications as per comments from Program Office.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-42951

Made modifications as per comments from Program Office.

V-42952

Made modifications as per comments from Program Office.

V-42953

Made modifications as per comments from Program Office.

V-42955

Made modifications as per comments from Program Office.

V-42956

Made modifications as per comments from Program Office.

V-42957

Made modifications as per comments from Program Office.

V-42958

Made modifications as per comments from Program Office.

Documentation Update

Made modifications as per comments from Program Office.

McAfee MOVE Multi-Platform OSS STIG, Version 1, Release 5

V-42964

Made modifications as per comment matrix from Program Office.

V-42965

Made modifications as per comments from Program Office.

V-42968

Made modifications as per comments from Program Office.

Modified Rule Title to reflect 20 files required to be maintained.

V-42971

Made modifications as per comments from Program Office.

V-42973

Made modifications as per comments from Program Office.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-42974

Made modifications as per comments from Program Office.

V-42976

Made modifications as per comments from Program Office.

V-42977

Made modifications as per comments from Program Office.

V-42978

Made modifications as per comments from Program Office.

V-42979

Made modifications as per comments from Program Office.

V-42981

Made modifications as per comments from Program Office.

V-42982

Made modifications as per comments from Program Office.

V-42983

Made modifications as per comments from Program Office.

V-42986

Made modifications as per comments from Program Office.

McAfee MOVE Overview , Version 1, Release 2

Documentation Update

Made modifications as per comments from Program Office.

McAfee VSE 8.8 Local Client STIG, Version 5, Release 10

V-42556

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

V-42559

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

V-42568

Removed requirement for Disable Scan Cache in On Demand Scan (ODS).

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-59365

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

McAfee VSE 8.8 Managed Client STIG, Version 5, Release 12

V-42523

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

V-42526

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

V-42535

Removed requirement for Disable Scan Cache in On Demand Scan (ODS).

V-59363

Updated to reflect changes issued by FRAGO 2 to TASKORD 14-0018.

Microsoft Internet Explorer 10 STIG, Version 1, Release 14

V-6228

Removed Blank Home Page requirement.

Microsoft Internet Explorer 11 STIG, Version 1, Release 10

V-46477

Added NA for SIPR.

V-46819

Added NA for SIPR.

Microsoft Office Access 2010 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Access 2010 STIG, Version 1, Release 9

V-26625

Removed requirement for disabling of UI.

Microsoft Office Access 2013 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Access 2013 STIG, Version 1, Release 3

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-26625

Removed requirement for disabling of UI.

Microsoft Office Excel 2010 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Excel 2010 STIG, Version 1, Release 10

V-26625

Removed requirement for disabling of UI.

Microsoft Office Excel 2013 Benchmark, Version 1, Release 3

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Excel 2013 STIG, Version 1, Release 5

V-26625

Removed requirement for disabling of UI.

Microsoft Office InfoPath 2010 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office InfoPath 2010 STIG, Version 1, Release 10

V-26625

Removed requirement for disabling of UI.

Microsoft Office InfoPath 2013 Benchmark, Version 1, Release 3

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office InfoPath 2013 STIG, Version 1, Release 4

V-26625

Removed requirement for disabling of UI.

Microsoft Office Outlook 2010 STIG, Version 1, Release 12

V-26625

Removed requirement for disabling of UI.

Microsoft Office Outlook 2013 Benchmark, Version 1, Release 5

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Outlook 2013 STIG, Version 1, Release 8

V-26625

Removed requirement for disabling of UI.

Microsoft Office PowerPoint 2010 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

V-26639

Updated OVAL impacted by removal of DTOO305.

Microsoft Office PowerPoint 2010 STIG, Version 1, Release 9

V-26625

Removed requirement for disabling of UI.

Microsoft Office PowerPoint 2013 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office PowerPoint 2013 STIG, Version 1, Release 4

V-26625

Removed requirement for disabling of UI.

Microsoft Office Publisher 2010 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Publisher 2010 STIG, Version 1, Release 10

V-26625

Removed requirement for disabling of UI.

Microsoft Office Publisher 2013 Benchmark, Version 1, Release 3

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Publisher 2013 STIG, Version 1, Release 4

V-26625

October 2016 STIGs to be Released

Release Date: October 28, 2016

Removed requirement for disabling of UI.

Microsoft Office Visio 2013 Benchmark, Version 1, Release 2

V-40743

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Visio 2013 STIG, Version 1, Release 32

V-40743

Removed requirement for disabling of UI.

Microsoft Office Word 2010 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Word 2010 STIG, Version 1, Release 10

V-26625

Removed requirement for disabling of UI.

Microsoft Office Word 2013 Benchmark, Version 1, Release 2

V-26625

Disabled Rule in OVAL corresponding to removal from STIG.

Microsoft Office Word 2013 STIG, Version 1, Release 4

V-26625

Removed requirement for disabling of UI.

Mobile Device Management (MDM) Server Policy STIG, Version 2, Release 4

V-24955

Updated check procedures based on current DoD policy.

V-24962

Updated Check Content.

V-24970

Removed references to Knox in the Check Content as the information is out-of-date.

V-24971

Removed requirement from the MDM Policy STIG as it is the responsibility of the local AO, not the CMD management server AO.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-28313

Removed references to Knox in the Check Content as the information is out-of-date.

Documentation Update

Changed STIG name from CMD Management Server Policy STIG to Mobile Device Management (MDM) Server Policy STIG.

Added Overview and Revision History documentation to the STIG package.

Mobile Policy STIG, Version 2, Release 3

V-8283

Updated all policy references and terminology throughout check.

V-8284

Removed from the Mobile Policy STIG as it is no longer required based on current DoD policy.

V-8297

Updated terminology in check (e.g., DAA).

V-12072

Removed from the Mobile Policy STIG. Requirement is related to SCIFs, DIA guidance applies, responsibility of DIA to review. The DSAWG directed similar requirements be removed from wireless STIGs several years ago. This is the first time the STIG has been updated since the DSAWG direction.

V-12106

Updated Check Content based on current DoD policy.

V-13982

Updated terminology in check (e.g., DAA).

V-14894

Removed from the Mobile Policy STIG as it is covered by the Network Infrastructure Policy STIG.

V-15782

Removed from the Mobile Policy STIG as it is no longer required based on current DoD policy.

V-19813

Updated terminology in Check Content (e.g., DAA).

Documentation Update

Added Overview and revision history to STIG package.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Mozilla Firefox STIG, Version 4, Release 16

V-15776

Changed policy to just disable saved passwords.

V-15777

Changed policy privacy.sanitize.timespan=40 days.

V-15990

Removed Blank Home Page requirement.

V-19741

Revised update source description.

V-19743

Revised incorrect sample file data.

V-64891

Updated to specify file may need to be created.

MS SQL Server 2012 Database STIG, Version 1, Release 12

V-41402

Trace definition code moved from Check to supplemental file.

V-41403

Supplied sample code, in a supplemental file.

V-41404

Supplied sample code, in a supplemental file.

V-41406

Supplied sample code, in a supplemental file.

V-41417

Modified Rule Title and Check Content to prevent a false positive.

V-70627

Added new requirement spun off from SQL2-00-017500.

MS SQL Server 2012 Instance STIG, Version 1, Release 12

V-40921

Deleted. SQL Server inherently meets the requirement.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-40932

Reworded to prohibit specification of unlimited growth of transaction log and for clarity.

V-41021

Trace definition code moved from Check Content to supplemental file.

V-41027

Trace definition code moved from Check Content to supplemental file.

V-41028

Trace definition code moved from Check Content to supplemental file.

V-41029

Trace definition code moved from Check Content to supplemental file.

V-41030

Trace definition code moved from Check Content to supplemental file.

V-41031

Trace definition code moved from Check Content to supplemental file.

V-41032

Trace definition code moved from Check Content to supplemental file.

V-41033

Trace definition code moved from Check Content to supplemental file.

V-41035

Trace definition code moved from Check Content to supplemental file.

V-41042

Trace definition code moved from Check Content to supplemental file.

V-41305

Trace definition code moved from Check Content to supplemental file.

V-41306

Trace definition code moved from Check Content to supplemental file.

V-41307

October 2016 STIGs to be Released

Release Date: October 28, 2016

Trace definition code moved from Check Content to supplemental file.

V-70625

Added new requirement to the STIG.

MS SQL Server 2014 Database STIG, Version 1, Release 2

V-67359

Provided more detail on how to identify and review audit definitions.

V-67365

Supplied sample code, in a supplemental file.

V-67367

Supplied sample code, in a supplemental file.

V-67369

Supplied sample code, in a supplemental file.

V-67377

Corrected the Vulnerability Discussion.

V-67385

Modified Rule Title, Vulnerability Discussion and Check Content to prevent a false positive.

Corrected the Vulnerability Discussion.

V-67391

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-67393

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-67395

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-67397

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-67399

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-67411

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

V-67413

Provided more detail on how to identify and review audit definitions.

V-67415

Provided more detail on how to identify and review audit definitions.

V-67417

Provided more detail on how to identify and review audit definitions.

V-67419

Provided more detail on how to identify and review audit definitions.

V-67421

Provided more detail on how to identify and review audit definitions.

V-67423

Provided more detail on how to identify and review audit definitions.

V-67425

Provided more detail on how to identify and review audit definitions.

V-67427

Provided more detail on how to identify and review audit definitions.

V-67429

Provided more detail on how to identify and review audit definitions.

V-67431

Provided more detail on how to identify and review audit definitions.

V-67433

Provided more detail on how to identify and review audit definitions.

V-67435

Provided more detail on how to identify and review audit definitions.

V-67437

October 2016 STIGs to be Released

Release Date: October 28, 2016

Provided more detail on how to identify and review audit definitions.

V-67439

Provided more detail on how to identify and review audit definitions.

V-67441

Provided more detail on how to identify and review audit definitions.

V-67443

Provided more detail on how to identify and review audit definitions.

MS SQL Server 2014 Instance STIG, Version 1, Release 3

V-67769

Provided more detail on how to identify and review audit definitions.

V-67771

Provided more detail on how to identify and review audit definitions.

V-67865

Removed requirement. SQL Server inherently meets the requirement.

V-67867

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

V-67887

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-67903

Provided more detail on how to identify and review audit definitions.

V-67917

Provided more detail on how to identify and review audit definitions.

V-67919

Provided more detail on how to identify and review audit definitions.

V-67921

Provided more detail on how to identify and review audit definitions.

V-67923

Provided more detail on how to identify and review audit definitions.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-67925

Provided more detail on how to identify and review audit definitions.

V-67927

Provided more detail on how to identify and review audit definitions.

V-67929

Provided more detail on how to identify and review audit definitions.

V-67931

Provided more detail on how to identify and review audit definitions.

V-67933

Provided more detail on how to identify and review audit definitions.

V-67935

Provided more detail on how to identify and review audit definitions.

V-67937

Provided more detail on how to identify and review audit definitions.

V-70623

Added new requirement to the STIG.

Network Device Management (NDM) SRG, Version 2, Release 7

V-55027

Changed discussion of administrator account so it is in compliance with local account of last resort.

V-55037

Changed "emergency administrative account" to "account of last resort". Also use the word local accounts so that this does not apply to authentication server account.

V-55041

Changed "emergency administrative account" to "account of last resort". Also use the word local accounts so that this does not apply to authentication server account.

V-55103

Changed emergency account to account of last resort in the Rule Title and Vulnerability Discussion. Added the local.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-55105

Updated the severity level to CAT 1 finding when a local account of last resort does not use an approved multifactor authentication method.

V-55113

Changed "emergency administrative account" to "account of last resort". Also use the word local accounts so that this does not apply to authentication server account.

V-55135

Changed "emergency administrative account" to "account of last resort". Also use the word local accounts so that this does not apply to authentication server account.

V-55139

Changed "emergency administrative account" to "account of last resort". Also use the word local accounts so that this does not apply to authentication server account.

V-55175

Changed "emergency administrative account" to "account of last resort". Also use the word local accounts so that this does not apply to authentication server account.

V-55187

Changed discussion of administrator account so it is in compliance with local account of last resort.

V-55299

Reworded to use and define "emergency account" consistent with 800-53, "account of last resort" instead of "administrative account", and local accounts so that it does not apply to authentication server account.

Network Devices STIG, Version 8, Release 20

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Network Firewall STIG - Cisco, Version 8, Release 20

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network Firewall STIG, Version 8, Release 20

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Network Infrastructure L3 Switch STIG - Cisco, Version 8, Release 21

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-5624

Updated example in Check Content.

V-14671

Added MD5 exception to Check Content section.

V-17833

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

Documentation Update

Synchronized release number, no other changes have been made.

Network Infrastructure L3 Switch STIG, Version 8, Release 21

V-3966

October 2016 STIGs to be Released

Release Date: October 28, 2016

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-5624

Updated example in Check Content.

V-14671

Added MD5 exception to Check Content section.

V-17833

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

Documentation Update

Synchronized release number, no other changes have been made.

Network Infrastructure Router STIG - Cisco, Version 8, Release 21

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network Infrastructure Router STIG - Juniper, Version 8, Release 21

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

October 2016 STIGs to be Released

Release Date: October 28, 2016

Synchronized release number, no other changes have been made.

Network Infrastructure Router STIG, Version 8, Release 21

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network IPSec VPN Gateway STIG, Version 1, Release 11

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Network Layer 2 Switch STIG - Cisco, Version 8, Release 20

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-5624

Updated example in Check Content.

V-14671

Added MD5 exception to Check Content section.

Network Layer 2 Switch STIG, Version 8, Release 20

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-5611

Added "log" to Check Content example.

V-5624

Updated example in Check Content.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network Perimeter L3 Switch STIG - Cisco, Version 8, Release 24

V-3028

Corrected Check Content and Fix Text Sections.

V-3077

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-5624

Updated example in Check Content.

V-14671

Added MD5 exception to Check Content section.

V-17833

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

Documentation Update

Synchronized release number, no other changes have been made.

Network Perimeter L3 Switch STIG, Version 8, Release 24

V-3028

Corrected Check Content and Fix Text Sections.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-5624

Updated example in Check Content.

V-14671

Added MD5 exception to Check Content section.

V-17833

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

Documentation Update

Synchronized release number, no other changes have been made.

Network Perimeter Router STIG - Cisco, Version 8, Release 24

V-3028

Corrected Check Content and Fix Text Sections.

V-3077

Updated Vulnerability Discussion, Check Content, and Fix Text sections.

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network Perimeter Router STIG - Juniper, Version 8, Release 24

V-3028

Corrected Check Content and Fix Text Sections.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network Perimeter Router STIG, Version 8, Release 24

V-3028

Corrected Check Content and Fix Text Sections.

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Documentation Update

Synchronized release number, no other changes have been made.

Network SRG, Version 2, Release 0.6

V-46089

Added CCI-000196 by reactivating SRG-NET-NA-000128 in the Network SRG.

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

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

October 2016 STIGs to be Released

Release Date: October 28, 2016

Added MD5 exception to Check Content section.

Network WLAN Access Point (Internet Gateway Only Connection) STIG

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Network WLAN Bridge STIG, Version 6, Release 12

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Network WLAN Controller STIG , Version 6, Release 12

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Network WMAN Access Point STIG , Version 6, Release 11

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Network WMAN Bridge STIG, Version 6, Release 11

V-3966

Updated Rule Title, Vulnerability Discussion, Check Content, and Fix Text sections.

V-5611

Added "log" to Check Content example.

V-14671

Added MD5 exception to Check Content section.

Oracle Database 11.2g STIG, Version 1, Release 9

V-52135

Modified mention of location of sqlnet.ora.

V-52145

Added warning: Do not attempt to encrypt SYSTEM table space.

V-52165

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-52177

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-52181

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-52207

Modified mention of location of sqlnet.ora.

V-52211

Modified mention of location of sqlnet.ora.

Added warning: Do not attempt to encrypt SYSTEM table space.

V-52217

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

Modified mention of location of sqlnet.ora.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-52237

Check modified for better alignment with requirement.

V-52255

Modified mention of location of sqlnet.ora.

V-52257

Modified mention of location of sqlnet.ora.

V-52259

Modified mention of location of sqlnet.ora.

V-52261

Modified mention of location of sqlnet.ora.

V-52265

Modified mention of location of sqlnet.ora.

V-52267

Modified mention of location of sqlnet.ora.

V-52285

Modified mention of location of sqlnet.ora.

V-52289

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

Modified mention of location of sqlnet.ora.

V-52293

Modified mention of location of sqlnet.ora.

V-52295

Modified mention of location of sqlnet.ora.

V-52331

Modified mention of location of sqlnet.ora.

V-52333

Modified mention of location of sqlnet.ora.

V-52351

October 2016 STIGs to be Released

Release Date: October 28, 2016

Reworded to remove conflict with V-52407. Added a finding statement to the Check Content.

V-52395

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-52397

Modified mention of location of sqlnet.ora.

V-52439

Modified mention of location of sqlnet.ora.

V-52465

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-53983

Check revised to avoid false positives and false negatives.

V-53987

Check Content revised to prevent false positives and false negatives.

V-53989

Check Content revised to prevent false positives and false negatives.

V-53995

Check Content revised to prevent false positives and false negatives.

V-53999

Corrected reference to Oracle documentation.

V-54011

Check Content revised to prevent false positives and false negatives.

V-54017

Check Content revised to prevent false positives and false negatives.

V-54047

Modified mention of location of sqlnet.ora.

V-54077

Modified mention of location of sqlnet.ora.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Oracle Database 12c STIG, Version 1, Release 5

V-61423

Obsolete requirement removed.

V-61433

Check Content revised to prevent false positives and false negatives.

V-61437

Check Content revised to prevent false positives and false negatives.

V-61439

Check Content revised to prevent false positives and false negatives.

V-61445

Check Content revised to prevent false positives and false negatives.

V-61461

Check Content revised to prevent false positives and false negatives.

V-61467

Check Content revised to prevent false positives and false negatives.

V-61515

Modified mention of location of sqlnet.ora.

V-61527

Modified Check Content query and Fix Text instructions.

V-61535

Modified mention of location of sqlnet.ora.

V-61543

Modified mention of location of sqlnet.ora.

V-61545

Modified mention of location of sqlnet.ora.

V-61559

Reworded to remove conflict with V-61603. Added a finding statement to the Check Content.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-61565

Modified Check Content query and Fix Text instructions.

V-61569

Modified Check Content query and Fix Text instructions.

V-61571

Modified Check Content query and Fix Text instructions.

V-61573

Modified Check Content query and Fix Text instructions.

V-61609

Modified mention of location of sqlnet.ora.

V-61611

Removed requirement as it is a duplicate of V-61811.

V-61667

Modified mention of location of sqlnet.ora.

Added warning: Do not attempt to encrypt SYSTEM table space.

V-61703

Modified mention of location of sqlnet.ora.

V-61705

Modified mention of location of sqlnet.ora.

V-61707

Modified mention of location of sqlnet.ora.

V-61709

Modified mention of location of sqlnet.ora.

V-61713

Modified mention of location of sqlnet.ora.

V-61715

Modified mention of location of sqlnet.ora.

V-61733

Modified mention of location of sqlnet.ora.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-61737

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed
Modified mention of location of sqlnet.ora.

V-61741

Modified mention of location of sqlnet.ora.

V-61743

Modified mention of location of sqlnet.ora.

V-61759

Modified mention of location of sqlnet.ora.

V-61765

Modified mention of location of sqlnet.ora.

V-61773

Added warning, "Do not attempt to encrypt SYSTEM table space".

V-61785

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

V-61791

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

V-61793

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

V-61811

Modified mention of location of sqlnet.ora.

V-61815

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.
Modified mention of location of sqlnet.ora.

V-61843

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-61845

Modified mention of location of sqlnet.ora.

V-61887

Added acknowledgment that DBA may have limited scope to address the issue, and advice on how to proceed

Oracle JRE 8 for Windows STIG, Version 1, Release 2

V-66939

Updated file location info.

V-66957

Fixed typo: "C:\ProgramFiles\Java\jre1.8.x.x\lib\exception.sites".
Added provision for DeploymentRuleSet.jar.

V-66959

Added provision for DeploymentRuleSet.jar.

Oracle Linux 5 STIG, Version 1, Release 8

V-775

Added wording to allow for less permissive permissions.

V-776

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-907

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11947

Added wording to the Check Content to verify that the minimum password length is set in /etc/login.defs.

V-11985

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11986

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22354

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-22355

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22359

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22360

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22363

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22364

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22409

Updated "timestamp_request" to "timestamp-request".

Oracle Linux 6 STIG, Version 1, Release 8

V-50791

Added wording to the Check Content to verify that the "minlen" password variable is set when `dam cracklib.so` is used.

V-50835

Updated Check Content to be more consistent with the Rule Title.

Red Hat 5 Benchmark, Version 1, Release 17

V-776

Removed a test from the OVAL that was no longer necessary and causing false positives.

V-794

Updated the OVAL to check the directories defined in the updated STIG requirement.

V-795

Updated the OVAL to check the directories defined in the updated STIG requirement.

V-796

Updated the OVAL to check the directories defined in the updated STIG requirement.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-924

Updated the OVAL to allow /dev/log to be world writable to match the STIG requirement.

V-932

Updated OVAL to fix the cause of the false negatives.

V-22302

Updated the OVAL in conjunction with GEN000590.

V-22303

Updated the OVAL to match the current STIG requirement.

V-22304

Updated the OVAL in conjunction with GEN000590.

V-22310

Updated the OVAL to match the updated STIG requirement.

Red Hat 5 STIG, Version 1, Release 16

V-775

Added wording to allow for less permissive permissions.

V-776

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-907

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11947

Added wording to the Check Content to verify that the minimum password length is set in /etc/login.defs.

V-11985

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11986

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22354

October 2016 STIGs to be Released

Release Date: October 28, 2016

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22355

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22359

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22360

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22363

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22364

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22409

Updated "timestamp_request" to "timestamp-request".

Red Hat 6 Benchmark, Version 1, Release 13

V-38469

Updated the OVAL to fix the cause of the false positives and negatives and work around the limitations of McAfee Policy Auditor.

V-38472

Enabled and updated the OVAL to work around the limitations of McAfee Policy Auditor.

V-38482

Updated OVAL to account for dual architecture systems.

V-38569

Updated OVAL to account for dual architecture systems.

V-38570

Updated OVAL to account for dual architecture systems.

V-38571

Updated OVAL to account for dual architecture systems.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-38572

Updated OVAL to account for dual architecture systems.

V-38687

Updated the OVAL to match the updated STIG requirement.

Red Hat 6 STIG, Version 1, Release 13

V-38475

Added wording to the Check Content to verify that the "minlen" password variable is set when `pam cracklib.so` is used.

V-38625

Removed the LDAP specific requirement from the STIG.

V-38626

Removed the LDAP specific requirement from the STIG.

V-38627

Modified the requirement to specifically disallow the installation of the `openldap-servers` package.

V-38641

Updated Check Content to be more consistent with the Rule Title.

V-38687

Updated package name from "openswan" to "libreswan".

Solaris 10 SPARC Benchmark, Version 1, Release 16

V-899

Updated the OVAL to properly handle netgroups.

V-22310

Updated the OVAL to match the updated STIG requirement.

V-22413

Updated OVAL to do checks in non-global zones with exclusive interfaces.

V-22414

Updated OVAL to do checks in non-global zones with exclusive interfaces.

V-22582

Updated OVAL to do checks in non-global zones with exclusive interfaces.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Solaris 10 SPARC STIG, Version 1, Release 16

V-776

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-808

Updated command in Check Content to focus strictly on home directories.

V-810

Updated Check Content to permit the existence of uucp accounts, if needed.

V-907

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-4269

Updated Check Content to permit the existence of uucp accounts, if needed.

V-4301

Updated Check Content and Fix Text to be zone-aware and to force the continuous use of NTP rather than a periodic time update.

V-4696

Updated Check Content to permit the existence of uucp accounts, if needed.

V-11985

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11986

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-12765

Updated file names in Check Content.

V-22291

Updated Check Content and Fix Text to be zone-aware and to force the continuous use of NTP rather than a periodic time update.

V-22292

Updated Check Content and Fix Text to be zone-aware and to force the continuous use of NTP rather than a periodic time update.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-22354

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22355

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22359

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22360

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22363

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22364

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22582

Updated Check Content and Fix Text to be zone-aware and to check for exclusive interface ownership for firewalls.

Solaris 10 x86 Benchmark, Version 1, Release 16

V-899

Updated the OVAL to properly handle netgroups.

V-4248

Updated OVAL identification of systems using ZFS root partition.

V-4249

Updated OVAL identification of systems using ZFS root partition.

V-22310

Updated the OVAL to match the updated STIG requirement.

V-22413

Updated OVAL to do checks in non-global zones with exclusive interfaces.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-22414

Updated OVAL to do checks in non-global zones with exclusive interfaces.

V-22582

Updated OVAL to do checks in non-global zones with exclusive interfaces.

Solaris 10 x86 STIG, Version 1, Release 16

V-776

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-808

Updated command in Check Content to focus strictly on home directories.

V-810

Updated Check Content to permit the existence of uucp accounts, if needed.

V-907

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-4269

Updated Check Content to permit the existence of uucp accounts, if needed.

V-4301

Updated Check Content and Fix Text to be zone-aware and to force the continuous use of NTP rather than a periodic time update.

V-4696

Updated Check Content to permit the existence of uucp accounts, if needed.

V-11985

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-11986

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-12765

Updated file names in Check Content.

V-22291

Updated Check Content and Fix Text to be zone-aware and to force the continuous use of NTP rather than a periodic time update.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-22292

Updated Check Content and Fix Text to be zone-aware and to force the continuous use of NTP rather than a periodic time update.

V-22354

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22355

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22359

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22360

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22363

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22364

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-22582

Updated Check Content and Fix Text to be zone-aware and to check for exclusive interface ownership for firewalls.

Solaris 11 SPARC Benchmark, Version 1, Release 4

V-48077

Updated the OVAL to match the updated STIG requirement.

V-48105

Disabled the rule in OVAL since updating the check would require OVAL version 5.11.

Solaris 11 SPARC STIG, Version 1, Release 9

V-47915

Updated requirement to permit the use of telnet in support of vntsd.

V-48023

October 2016 STIGs to be Released

Release Date: October 28, 2016

Updated Check Content to account for an edge case of nx* used with ASLR to be a finding.

V-48037

Updated Check Content to remove extraneous backslash character in the command.

V-48077

Updated Check Content to include sshd account as permissible.

V-59831

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-59833

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-59835

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-59837

Updated Check Content to look at all "rc" scripts as well for world-writable files.

V-71495

Added new requirement to restrict use of vntsd to specific roles.

V-71497

Added new requirement regarding configuration of vntsd authorization.

Solaris 11 x86 Benchmark, Version 1, Release 4

V-48077

Updated the OVAL to match the updated STIG requirement.

V-48105

Disabled the rule in OVAL since updating the check would require OVAL version 5.11.

Solaris 11 x86 STIG, Version 1, Release 9

V-47915

Updated requirement to permit the use of telnet in support of vntsd.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-48023

Updated Check Content to account for an edge case of nx* used with ASLR to be a finding.

V-48037

Updated Check Content to remove extraneous backslash character in the command.

V-48077

Updated Check Content to include sshd account as permissible.

V-59831

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-59833

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-59835

Adjusted wording to allow for vendor defined paths, and relative paths authorized by an ISSO.

V-59837

Updated Check Content to look at all "rc" scripts as well for world-writable files.

SUSE Linux Enterprise Server (SLES) v11 for System z STIG, Version 1,

V-11990

Updated Check Content. Changed "1002" to "-1002" which will include a wildcard.

V-22506

Updated Check Content. Added "unless the changes were made due to another STIG entry" to the end of the requirement.

V-22575

Removed requirement. There are requirements already in place that protect/defend against the identified characteristics.

Tanium 6.5 STIG, Version 1, Release 2

V-66975

Correction to "sign_all_questions" directive.

V-66983

Correction to Rule Title regarding directory restriction to SYSTEM.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-67013

Correction to verification steps to be on Tanium server and not Tanium Module Server.

V-67015

Correction to verification steps to be on Tanium server and not Tanium Module Server.

V-67017

Correction to verification steps to be on Tanium server and not Tanium Module Server.

V-67051

Correction to variable to validate.

V-67063

Correction to Rule Title to accurately reflect variable being validated.

Modification to allowed/restricted algorithms.

V-67073

Correction to reflect a "true" variable as not a finding.

Correction to fix verbiage regarding contacting Tanium for updated license.

V-67111

Correction to Rule Title to accurately reflect variable being validated.

Voice Video Endpoint SRG, Version 1, Release 3

V-66697

Removed SRG-NET-000371-VVEP-00008 (V-66697) as MACsec is no longer a requirement for Voice Video Endpoints.

V-71671

Added SRG-NET-000412-VVEP-00065 to require Voice Video Endpoints be in compliance with CNSSI 5000.

Voice Video Session Management SRG, Version 1, Release 2

V-71683

Added SRG-NET-000512-VVSM-00054 to obfuscate passwords within configuration files.

V-71685

Added SRG-NET-000343-VVSM-00055 to require authentication of Voice Video trunks.

V-71687

Added SRG-NET-000338-VVSM-00056 to require re-registration of Voice Video trunks.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-71689

Added SRG-NET-000512-VVSM-00057 to require Voice Video Session Managers be in compliance with CNSSI 5000.

Windows 10 Benchmark, Version 1, Release 4

V-63395

Updated OVAL to match the updated STIG requirement, which includes the new McAfee Agent Service name.

V-63529

Disabled the rule in OVAL because it is being removed from the STIG.

V-63579

Updated OVAL to reference new certificate requirements.

V-63583

Updated OVAL to reference new certificate requirements.

V-63587

Updated OVAL to reference new certificate requirements.

V-63589

Updated OVAL to reference new certificate requirements.

V-63601

Added new OVAL for the requirement.

V-63611

Added new OVAL for the requirement.

V-63619

Added new OVAL for the requirement.

V-63625

Added new OVAL for the requirement.

V-63699

Updated the OVAL to work with Windows 10 Enterprise LTSB.

V-63701

Updated the OVAL to work with Windows 10 Enterprise LTSB.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-63705

Updated the OVAL to work with Windows 10 Enterprise LTSC.

V-63709

Updated the OVAL to work with Windows 10 Enterprise LTSC.

V-63713

Updated the OVAL to work with Windows 10 Enterprise LTSC.

V-68817

Added new OVAL content.

V-68819

Added new OVAL content.

V-68821

Added new OVAL content.

V-70637

Added new OVAL for the requirement.

V-70639

Added new OVAL for the requirement.

Windows 10 Mobile STIG, Version 1, Release 2

V-70107

Revised Check Content and Fix Text due to OS update.

V-70133

Revised Check Content and Fix Text due to OS update.

V-70139

Revised Check Content and Fix Text due to OS update.

V-70141

Removed requirement as it is no longer needed due to OS update.

V-71681

Added new requirement to require anniversary OS update to be installed.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Documentation Update

Updated technical content in Configuration Tables and Supplemental documents due to anniversary update of OS.

Windows 10 STIG, Version 1, Release 6

V-63327

Removed firmware related requirement as outside of OS scope.

V-63331

Removed firmware related requirement as outside of OS scope.

V-63395

Updated for v5 of McAfee agent.

V-63521

Clarified requirement for location of Windows Error Reporting data.

V-63529

Removed Windows Error Reporting port requirement, not security related.

V-63579

Updated PKE related requirement with current certificates.

V-63583

Updated PKE related requirement with current certificates.

V-63587

Updated PKE related requirement with current certificates.

V-63589

Updated PKE related requirement with current certificates.

V-70637

Added requirement to remove legacy feature PowerShell 2.0 from the system.

V-70639

Added requirement to remove legacy feature SMB 1.0 from the system.

Windows 2008 DC Benchmark, Version 6, Release 36

V-26604

Added new OVAL content.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-26605

Added new OVAL content.

V-26606

Added new OVAL content.

V-32272

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

Windows 2008 DC STIG, Version 6, Release 34

V-2376

Clarified location of Kerberos policy.

V-2377

Clarified location of Kerberos policy.

V-2378

Clarified location of Kerberos policy.

V-2379

Clarified location of Kerberos policy.

V-2380

Clarified location of Kerberos policy.

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

October 2016 STIGs to be Released

Release Date: October 28, 2016

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-56511

Clarified Windows Error Reporting service requirement on server core installations.

V-57457

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

Windows 2008 MS Benchmark, Version 6, Release 36

V-26604

Added new OVAL content.

V-26605

Added new OVAL content.

V-26606

Added new OVAL content.

V-32272

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

Windows 2008 MS STIG, Version 6, Release 34

V-15505

October 2016 STIGs to be Released

Release Date: October 28, 2016

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-56511

Clarified Windows Error Reporting service requirement on server core installations.

V-57457

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

Windows 2008 R2 DC Benchmark, Version 1, Release 22

V-26604

Added new OVAL content.

V-26605

Added new OVAL content.

V-26606

Added new OVAL content.

V-32272

Updated OVAL to reference new certificate requirements.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

Windows 2008 R2 DC STIG, Version 1, Release 20

V-2376

Clarified location of Kerberos policy.

V-2377

Clarified location of Kerberos policy.

V-2378

Clarified location of Kerberos policy.

V-2379

Clarified location of Kerberos policy.

V-2380

Clarified location of Kerberos policy.

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-56511

Clarified Windows Error Reporting service requirement on server core installations.

V-57457

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

Windows 2008 R2 MS Benchmark, Version 1, Release 23

V-1155

Updated the OVAL to match the updated STIG requirement.

V-26604

Added new OVAL content.

V-26605

Added new OVAL content.

V-26606

Added new OVAL content.

V-32272

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

Windows 2008 R2 MS STIG, Version 1, Release 20

V-1155

Updated to allow "Local account and member of Administrators group".

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-56511

Clarified Windows Error Reporting service requirement on server core installations.

V-57457

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

Windows 2012/2012 R2 DC Benchmark, Version 2, Release 6

V-32272

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

Windows 2012/2012 R2 DC STIG, Version 2, Release 6

V-1163

Removed data in False Positive field, duplicated in Check.

V-1164

Removed data in False Positive field, duplicated in Check.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-3245

Removed data in False Positive field, duplicated in Check.

V-3383

Removed data in Potential Impacts field, duplicated in Check.

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-36667

Clarified for virtual machines and systems with network attached storage.

V-36668

Clarified for virtual machines and systems with network attached storage.

V-40193

Removed requirement for virtual machine asset registration. Policy outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-56511

Clarified Windows Error Reporting service requirement on server core installations.

V-57457

Clarified requirement for location of Windows Error Reporting data.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-57461

Removed Windows Error Reporting port requirement, not security related.

V-57655

Clarified requirement based on GPOS SRG update.

Windows 2012/2012 R2 MS Benchmark, Version 2, Release 6

V-1155

Updated the OVAL to match the updated STIG requirement.

V-32272

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

Windows 2012/2012 R2 MS STIG, Version 2, Release 6

V-1155

Updated to allow "Local account and member of Administrators group".

V-1163

Removed data in False Positive field, duplicated in Check.

V-1164

Removed data in False Positive field, duplicated in Check.

V-3245

Removed data in False Positive field, duplicated in Check.

V-3383

Removed data in Potential Impacts field, duplicated in Check.

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-36667

Clarified for virtual machines and systems with network attached storage.

V-36668

Clarified for virtual machines and systems with network attached storage.

V-40193

Removed requirement for virtual machine asset registration. Policy outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-56511

Clarified Windows Error Reporting service requirement on server core installations.

V-57457

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

V-57655

Clarified requirement based on GPOS SRG update.

Windows 7 Benchmark, Version 1, Release 30

V-32272

Updated the OVAL to match the updated STIG requirement.

V-32273

October 2016 STIGs to be Released

Release Date: October 28, 2016

Updated OVAL to reference new certificate requirements.

V-32274

Updated the OVAL to match the updated STIG requirement.

V-40237

Updated the OVAL to match the updated STIG requirement.

Windows 7 STIG, Version 1, Release 24

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32273

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-57457

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

Windows 8/8.1 Benchmark, Version 1, Release 16

V-32272

Updated OVAL to reference new certificate requirements.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-32273

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

V-40237

Updated OVAL to reference new certificate requirements.

V-43239

Added new OVAL content.

Windows 8/8.1 STIG, Version 1, Release 15

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32273

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

V-43243

Updated for application name change to OneDrive.

V-57457

October 2016 STIGs to be Released

Release Date: October 28, 2016

Clarified requirement for location of Windows Error Reporting data.

V-57461

Removed Windows Error Reporting port requirement, not security related.

Windows Firewall Benchmark, Version 1, Release 5

V-17424

Disabled Rule in OVAL corresponding to removal in STIG.

V-17434

Disabled Rule in OVAL corresponding to removal in STIG.

V-17444

Disabled Rule in OVAL corresponding to removal in STIG.

Benchmark Update

Updated the OVAL to include the necessary and correct CPE information to work on Windows 10.

Windows Firewall STIG, Version 1, Release 5

V-17424

Removed requirement defining firewall log location and file name.

V-17434

Removed requirement defining firewall log location and file name.

V-17444

Removed requirement defining firewall log location and file name.

Documentation Update

Updated Overview to clarify Windows Firewall is only required when HBSS Firewall cannot be used.

Windows Vista Benchmark, Version 6, Release 44

V-32272

Updated OVAL to reference new certificate requirements.

V-32273

Updated OVAL to reference new certificate requirements.

V-32274

Updated OVAL to reference new certificate requirements.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-40237

Updated OVAL to reference new certificate requirements.

Windows Vista STIG, Version 6, Release 41

V-4107

Added requirement warning of end support.

V-15505

Updated for v5 of McAfee agent.

V-32272

Updated PKE related requirement with current certificates.

V-32273

Updated PKE related requirement with current certificates.

V-32274

Updated PKE related requirement with current certificates.

V-36663

Removed BIOS related requirement as outside of OS scope.

V-36664

Removed BIOS related requirement as outside of OS scope.

V-40195

Removed BIOS related requirement as outside of OS scope.

V-40237

Updated PKE related requirement with current certificates.

z/OS ACF2 STIG, Version 6, Release 29

V-181

Updated to allow Security Administrators access to TSO Operator privilege.

V-7485

Updated for clarification of System Consoles.

V-65647

Corrected password encryption parameter spelling - PSWDENCT.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-71223

Added new requirement for REXX LIB.

Documentation Update

Added BMC MAINVIEW Resources for DB2 to addendum.

Added resources to SDSF Table.

Updated BPX.SMF Parameter.

Added note in Addendum referencing ESM.

Modified the Cross Reference spreadsheet to specify PCSPAUDI over PCSCAUDI on several resource

Modified the Cross Reference spreadsheet to add additional BMC Mainview for DB2 resources.

Modified the Cross Reference spreadsheet adding new SDSF resources.

Modified the Cross Reference spreadsheet adding new CA1 resource.

Modified the Cross Reference spreadsheet adding new SYSREX library dataset access requirements.

z/OS CA 1 Tape Management for ACF2 STIG , Version 6, Release 5

V-16932

Updated wording for datasets to be protected.

V-17985

Removed reference to DISA Field Security Office review - Require OA Approval.

z/OS CA 1 Tape Management for RACF STIG , Version 6, Release 5

V-16932

Updated wording for datasets to be protected.

V-17985

Removed reference to DISA Field Security Office review - Require OA Approval.

z/OS CA 1 Tape Management for TSS STIG , Version 6, Release 5

V-16932

Updated wording for datasets to be protected.

V-17985

Removed reference to DISA Field Security Office review - Require OA Approval.

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

Documentation Update

Updated CICS resources in Addendum.

October 2016 STIGs to be Released

Release Date: October 28, 2016

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

Documentation Update

Updated CICS resources in Addendum.

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

Documentation Update

Updated CICS resources in Addendum.

z/OS RACF STIG, Version 6, Release 29

V-290

Updated to Added note" For complete requirements for SMS-managed Values please review the ZSMSxxxx suite of requirement.

V-298

Corrected typo. Should be '**' instead of '*'.

V-7485

Updated for clarification of System Consoles.

V-71203

Added new requirement for default LOGOPTIONS.

V-71223

Added new requirement for REXX LIB.

Documentation Update

Added BMC MAINVIEW Resources for DB2 to addendum.

Added resources to SDSF Table.

Updated BPX.SMF Parameter.

Changed the Cross Reference spreadsheet to specify PCSPAUDT over PCSCAUDT on several resource.

Changed the Cross Reference spreadsheet adding new SDSF resources.

Changed the Cross Reference spreadsheet to add additional BMC Mainview for DB2 resources.

Changed the Cross Reference spreadsheet adding new CA1 resource.

Changed the Cross Reference spreadsheet adding new SYSREX library dataset access requirements.

Added note in Addendum referencing ESM.

z/OS SRR Scripts, Version 6, Release 29

V-36

Changed scripts to add automation on the question that is specified for the CSVDYLPA.ADD and CSVDYLPA.DELETE resources.

October 2016 STIGs to be Released

Release Date: October 28, 2016

V-181

Updated script to allow Security Administrators access to TSO OPERATOR privilege.

V-199

Changed script value for INACTIVE control.

V-6933

Changed script to specify PCSPAUDT over PCSCAUDT.

V-7485

Modified to clarify System Consoles.

V-17947

Changed scripts to evaluate new SDSF resources.

Changed scripts to add additional BMC Mainview for DB2 resources.

V-71203

Changed scripts to add new vulnerability for default LOGOPTIONS.

V-71223

Changed scripts to add new vulnerability for SYSREXX library dataset access.

SRR Script Update

Corrected access violations when generating DSNLIST information for RACF System REXX dataset containing the password REXX.

Corrected access violations when generating DSNLIST information from the MVSXRPT member within the EXAM.RPT dataset.

Corrected possible false finding for Logon IDs that have more specific permission that prevents access.

z/OS TSS STIG, Version 6, Release 29

V-199

Changed value for INACTIVE control.

V-7485

Updated for clarification of System Consoles.

V-71223

Added new requirement for REXX LIB.

Documentation Update

Added BMC MAINVIEW Resources for DB2 to addendum.

Added resources to SDSF Table.

October 2016 STIGs to be Released

Release Date: October 28, 2016

Updated BPX.SMF Parameter.

Changed the Cross Reference spreadsheet to specify PCSPAUDT over PCSCAUDT on several resource.

Changed the Cross Reference spreadsheet adding new SDSF resources.

Changed the Cross Reference spreadsheet to add additional BMC Mainview for DB2 resources.

Changed the Cross Reference spreadsheet adding new CA1 resource.

Changed the Cross Reference spreadsheet adding new SYSREX library dataset access requirements.

Added note in Addendum referencing ESM.