Evaluate-STIG ChangeLog

1.2404.0

May 14, 2024

What's New

- `-Output` can now include "Console" as an output option. This is also the default output. Allows outputting to both checklist files and console for the same scan.
- `-PreviousToKeep` now will retain all previous results when a negative value is used (e.g. `-PreviousToKeep -1`)
- Add support for ArcGIS Server 10.3 STIG
- Add support for Canonical Ubuntu 22.04 STIG
- Add support for Microsoft Exchange 2019 Edge Server
- Add support for Microsoft Exchange 2019 Mailbox Server
- Add support for Rancher Government Solutions RKE2 STIG

Other Changes

- Add MD5 Hash for Discussion, Check Text, and Fix Text. This is to assist internal development.
- Add GPG Fingerprint checks to RHEL/Oracle Modules (issue 1592)
- Add checks for RHEL8 V-230224,RHEL9 V-257879,Oracle8 V-248525 (issue 1591)
- Add checks for RHEL8 V-230229,RHEL9 V-258131,Oracle8 V-248531 (issue 1590)
- Add `New-ValidationObject` function that can be called from answer files for `<ValidationCode>` formatting (issue 1524)
- Improve Cisco Router Detection (issue 1586)
- Improve to better handle characters that were not rendering properly in output checklists (issue 1573)
- Improve querying of Active Directory group membership (issue 1567)
- Improve `Test-Prerequisites.bat` Execution Policy Checks (issue 1561)
- Improve user profile selection (issue 1554)
- Update filename timestamps to use 24 hour format instead of 12 hour (issue 1578)
- Update for Active Directory Domain STIG V3R4
- Update for Apache Server 2.4 Unix Server STIG V2R7
- Update for Canonical Ubuntu 18.04 LTS STIG V2R14
- Update for Canonical Ubuntu 20.04 LTS STIG V1R12
- Update for Cisco IOS XE Switch NDM STIG V2R9
- Update for JBoss EAP 6.3 STIG V2R4
- Update for Microsoft .Net Framework 4 STIG V2R4
- Update for Microsoft Excel 2016 V2R1
- Update for MS Edge STIG V1R8
- Update for MS Office 365 ProPlus STIG V2R12
- Update for MS Office System 2016 STIG V2R3
- Update for MS SQL Server 2016 Instance STIG V2R12
- Update for MS SQL Server 2016 Database STIG V2R9
- Update for Oracle Linux 8 V1R10
- Update for Red Hat Enterprise Linux 8 STIG V1R14
- Update for Red Hat Enterprise Linux 9 STIG V1R3
- Update for Windows 10 STIG V2R9
- Update for Windows 11 STIG V1R6
- Update for Windows Server 2016 STIG V2R8

- Update for Windows Server 2019 STIG V2R9
- Update for Windows Server 2022 STIG V1R5
- **Bug fixes:**
  - Issue 1624 : RHEL9 - V-258236 - Open and NotAFinding backwards
  - Issue 1613 : Tomcat STIG Scan check V-222979 resulting in Not_Reviewed status due to error caused by incorrect folder specified in the DISA STIG Check Text
  - Issue 1589 : Windows Server 2019/2022 V-205657/V-254239 Should be NA on DCs
  - Issue 1582 : Evaluate STIG 1.2401.3 Issues with RedHat 9 Checks
  - Issue 1579 : Multiple V-IDs 'grep' waiting for STDIN
  - Issue 1577 : Apache 2.4 UNIX Site STIG V-214300 check fails because of quotes around the SSLCACertificateFile directive
  - Issue 1575 : Remote Scan of Linux machine fails when using -ForceSTIG
  - Issue 1572 : AD Forest CKLs contain no CCI information
  - Issue 1570 : Incorrect parsing of command output in Get-VirtualHosts when NameVirtualHost directive is set
  - Issue 1569 : Incorrectly Parsing Audit Rules V-219296
  - Issue 1563 : RHEL8 V-244531 and RHEL7 V-204473 false negative
  - Issue 1562 : Modules for Older STIGs are Missing CCI References
  - Issue 1559 : Eval STIG Performing Apache Site Checks
  - Issue 1553 : Tomcat Potential False Positive V-222973 and V-223003
  - Issue 1552 : 222979 should check if the manager app is absent and report NF
  - Issue 1550 : V-213900 returning inconsistent results in 2401.3, possibly due to DB name
  - Issue 1549 : V-213901 local code issue starting with 2401.3, possibly due to DB name
  - Issue 1548 : V-205723 - Check reports NA on DC, but check should be applicable ONLY to DC
  - Issue 1546 : V-205740 - False-Positive for Default ACL missing when other account granted permission to SysVol
  - Issue 1543 : ADForest Module Missing CCI Data in Description Blocks
  - Issue 1542 : AnswerKey based on hostname does not appear to be working for 1.2401.3
  - Issue 1539 : AIDE false NOT A FINDING assignment due to incorrect text comparison check (RHEL7 V-251705 / RHEL8 V-251710)
  - Issue 1536 : Using -OutputPath yields "Error: The given path's format is not supported"
  - Issue 1535 : Evaluate-STIG generates multiple Tomcat checklists but fails to populate the Server number in field WEB_DB_SITE
  - Issue 1532 : SQL2016DB V-213902 no finding details if run remotely
  - Issue 1525 : When OutputPath is specified, it does not create non-existent directory
  - Issue 1444 : IIS 10 Site V-218779, V218780 - not scanning virtual directories in applications
  - Issue 1363 : RHEL 8 V-230279 false positive
  - Issue 1309 : SQL Instance 2016 V-213966 False Positive