CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Nessus Network Monitor 6.3.2

Maintenance Report Number: CCEVS-VR-VID11369-2025

Date of Activity: May 8, 2025

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Protection Profile for Application Software, Version 1.4, 7 October 2021 ([APP_PP])

Impact Analysis Report for Tenable Nessus Network Monitor, version 1.10, April 15, 2025

Nessus Network Monitor 6.3.2 Security Target Version 1.0, 31 March 2025

Tenable Nessus Network Monitor 6.3.x User Guide, 08 May 2025

Assurance Continuity Maintenance Report:

Leidos, Inc., submitted an Impact Analysis Report (IAR), on behalf of Tenable, Inc., for the changes from the certified TOE, Tenable Nessus Network Monitor 6.2.2 to Tenable Nessus Network Monitor 6.2.3. This was accomplished per the requirements of the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on April 15, 2025. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Reevaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target (ST), the User Guidance Documentation, and the Impact Analysis Report (IAR).

As a result, the following changes were made to the evaluation evidence:

1. Security Target – The Security Target has been updated to expand support for RHEL 8.7 up to 8.10 and for Windows Server 2019 up to 2022, and to update the CAVP certificate from A3617 to A6737.
2. Guidance Document – The Guidance Document was updated to reflect title and reference information.

Documentation Updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Tenable Nessus Network Monitor 6.2.2 Security Target, Version 1.1, 28 June 2023	**New Security Target:** Tenable Nessus Network Monitor 6.3.2 Security Target, Version 1.0, 31 March 2025
Common Criteria Compliance Guide: Tenable Nessus Network Monitor 6.2.x User Guide, 18 May 2023	**Maintained Common Criteria Compliance Guide:** Tenable Nessus Network Monitor 6.3.x User Guide, 08 May 2025

Changes to TOE:

The Nessus Network Monitor is substantially the same between versions 6.2.2 and 6.3.2. with support for the latest build of RHEL 8.10 and Windows Server 2022. The only differences are patches made to address specific published vulnerabilities, as well as minor functionality improvements and bug fixes that do not affect security functionality. Third party libraries were updated to address vulnerabilities; Nessus Network Monitor firmware was updated to address vulnerabilities and bugs; and the guidance documentation was updated for clarity and to add extra information for users and to reflect changed title and reference information. All changes were minor and had no impact on the security functionality.

Description of Regression Testing:

The developer performed regression testing on the TOE to ensure security functionality was not impacted by product updates. Automatic regression tests include comparing results of traffic data with the previous NIAP release, functional testing for memory usage using memory debuggers, long term memory leak system testing of 6.3. for 2 weeks or more, automatic upgrade testing, functional testing with other Tenable products, and UI and back end testing.

NIST CAVP Certificates:

The CAVP certificate was also updated (from A3617 To A6737) to expand support for RHEL 8.7 up to 8.10 and for Windows Server 2019 up to 2022. The original TOE was tested on virtualized instances of

Windows Server 2019 and RHEL 8.7, each running on VMware ESXi 6.5 on a system using an AMD Ryzen Threadripper 1950X processor. The necessary evaluation evidence was provided in the IAR.

Vulnerability Assessment:

The IAR contains the output from the vulnerability search conducted on 7 May 2025, as well as the rationale why the vulnerabilities identified in the search results are not applicable to the TOE.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), US-CERT (http://www.kb.cert.org), and the Tenable Security Advisories (https://www.tenable.com/security) using the 36 search terms below.

Search Term

- "c-ares 1.33.1"
- "chosen 1.8.7"
- "curl 8.12.0"
- "d3 3.4.8"
- "dpdk 20.08.0"
- "libexpat 2.7.0"
- "hyperscan 5.4.2"
- "libbacktrace 1.0"
- "libbzip2 1.0.8"
- "libpcap 1.10.5"
- "libpcre 8.45"
- "libxml2 2.13.7"
- "libxslt 1.1.41"
- "libxmlsec 1.3.2"
- "zlib 1.3.1"
- "openssl 3.0.16"
- "sqlite 3.40.1"
- "npcap 1.72"
- "libjpeg 9e"
- "Handlebars 4.7.8"
- "jQuery 3.6.4"
- " jQuery FileUpload 10.8.0"
- "jquery hotkeys 0.1.0"
- "jquery.iframe-transport.js 1.7"
- "jquery scrollto 2.1.3"
- "jquery storage api 1.7.3"
- "jquery tablesorter 0.11"
- "jquery-tooltip 0.2.1"
- "jQuery UI 1.13.2"
- "jquery.ui.touch-punch.min.js 0.2.3"
- "spin.js 1.2.5"
- "sugar 1.3"
- "mobile-detect.js 1.4.5"
- "Moment 2.29.4"
- "xml2json 0.9"
- "DataTables 1.13.6" .

The search yielded zero (0) matching for 31 of the search terms and 5 terms with one (1) matching record. Of these 5, the TOE was not vulnerable to any. These results of the vulnerability assessment were included in the IAR. No new vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

The update to OpenSSL, changes in TOE environment, do not affect the security claims of the Tenable Nessus Network Manager 6.3.2 Security Target.

This update results in no changes to SFRs, Security Functions, Assumptions or Objectives, or Assurance Documents. TOE Environment was changed, updating the platforms to a more modern version to support the latest build in RHEL's case, and to address Windows Server 2019 drop in official support. No additional functionality was added and therefore is a **minor** change. The security target and the Common Criteria Evaluation Guidance Document are updated to reflect the software minor version update.

Tenable obtained updated CAVP certificates covering the change in OpenSSL library (A6737).

Finally, the evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. The search did not identify any new potential vulnerability.

Validation Team Conclusion:

The validation team reviewed the changes, and concur the changes are **minor**, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The TOE has been updated from version 6.2.2 to 6.3.2 to account for the platform update to the latest build of RHEL Linux, and to address Windows Server 2019 drop in official support. Third party libraries were updated to address vulnerabilities; Nessus Network Monitor firmware was updated to address vulnerabilities and bugs; and the guidance documentation was updated for clarity and to add extra information for users and to reflect changed title and reference information. All changes were minor and had no impact on the security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.