# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Tenable Security Center 6.2.2

## Maintenance Update of Tenable Security Center 6.2.2

**Maintenance Report Number:** CCEVS-VR-VID11374-2025

**Date of Activity**: November 25, 2025

**References:**

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 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
- Tenable Security Center 6.2.0 Security Target, Version 1.1, 10 October 2023
- Tenable Security Center 6.2.2 Security Target, Version 1.1, 20 November 2025
- Tenable Security Center Impact Analysis Report, Version 1.1, 20 November 2025
- Tenable Security Center 6.2.2 Release Notes (2025-08-26)

## Evaluated TOE

- **VR Title** – Common Criteria Evaluation and Validation Scheme Validation Report for Tenable Security Center 6.2.0
- **VR Report #: CCEVS-VR-VID11374-2023**
- **VR Version** – 1.0
- **VR Date** –October 12, 2023

## Current AM TOE Updated

- **ACMR Title** – Common Criteria Evaluation and Validation Scheme Validation Report Senetas Distributed by Thales CN Series Encryptors 5.5.1
- **ACMR Report #: CCEVS-VR-VID11374-2025**
- **ACMR Version** – 1.0
- **ACMR Date** – November 25, 2025

## Documentation Updated:

| CC Evidence | Evidence Change Summary |
|---|---|
| Tenable Security Center 6.2.0 Security Target, Version 1.1, 10 October 2023. | Tenable Security Center 6.2.2 Security Target, Version 1.1, 20 November 2025<br>Updates include title page and relevant sections (e.g., TOE Identification, Cryptographic Support, and CAVP certificate details) have been updated. |
| **Guidance Documentation**:<br>Tenable Security Center 6.2.0 Common Criteria Evaluated Configuration Guide, 4 September 2023. | Tenable Security Center 6.2.2 Common Criteria Evaluated Configuration Guide (CCECG)<br>Last Revised: September 09, 2025.<br>Updates include Title page, ST Reference, TOE Reference, Document Purpose and Scope, Overview of the Target of Evaluation, Evaluated Configuration Updated TOE version to 6.2.2. |

## Assurance Continuity Maintenance Report:

Leidos, Inc. submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 25 September 2025. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. 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 consists of the Security Target, Administrative Guidance, and the IAR. The ST and Administrative Guidance documents were updated.

## Product Updates

All changes to the product, shown in the following table, were feature enhancements and have been assessed as minor. These enhancements do not affect the security functionality or claims of the previously evaluated TOE.

| Feature | Description | Impact Analysis |
|---|---|---|
| Updating OpenSSL to version 3.0.16 | OpenSSL has been updated to version 3.0.16 to implement vulnerability fixes provided by OpenSSL’s developer. | Minor — The version update does not add, remove, or modify any existing security functionality, as it was updated to address several vulnerabilities related to the previous version. |

| | | |
|---|---|---|
| Updating TOE environment to RHEL 8.10 | The TOE environments were updated from RHEL 8.7 to RHEL 8.10. | Minor — No change has been made to security functionality. The environment update was done to support RHEL's latest builds. No additional features or functions were added. |

## Development Environment Changes

There are no updates to development environment identified.

## Regression Testing

The following table describes the regression testing performed by the developer on the TOE to ensure security functionality was not impacted by product updates. These test activities cover the functionality of the entire product, which includes the subset of security functionality (e,g., authentication, encryption of data, secure communication) relevant to the evaluated TOE.

| **Tests** | **No of Tests (PO/P1 Testcases)** |
|---|---|
| Automation Testing: Minimal Acceptance Tests API Test, Basic UI Tests, Integration Tests | 390 |
| Functional manual testing on a fresh instance of SC 6.2.2 | 50 |
| Upgrade test: Setup an SC 6.2.1 GA instance and attempt an upgrade to SC 6.2.2 | Upgrade Completed Successfully |
| Functional manual testing on an instance upgraded from SC 6.2.1 -> SC 6.2.2 | 50 |
| Unit Tests as part of the build pipeline | 15000 |

## NIST Certificates:

The Security Center software is substantially the same between versions 6.2.0 and 6.2.2. The only differences are patches made to address specific published vulnerabilities and new features described in the product updates section of this ACMR, which are all categorized as minor changes.

Even though the updated TOE uses a revised OpenSSL version (3.0.16) and has an updated operational environment (e.g., a newer RHEL version), the CAVP certificate (A6737) confirms that the cryptographic module still meets all assurance requirements as the original evaluation.

## Vulnerability Assessment:

An updated vulnerability analysis was performed on 09 September 2025 and again on 20 November 2025 using the original search terms. None of the vulnerabilities discovered through public searches affect the evaluated TOE. There are no residual vulnerabilities in the new version of the product.

## Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the product changes and vulnerability updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.