ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Veeam ONE v12.3

Veeam ONE v12.3

Maintenance Report Number: CCEVS-VR-VID11371-2025
Date of Activity: 11 August 2025
References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, September 12, 2016
- *Veeam ONE v12 Impact Analysis Report*, Version 1.0, 17 July 2025
- *Veeam ONE v12 Security Target*, Version 1.7, 7 July 2025
- *Veeam ONE v12 Common Criteria Evaluated Configuration Guide (CCECG),* Version 1.1, July 8, 2025
- *Veeam ONE Version 12 Quick Start Guide*, July, 2025
- *Veeam ONE Version 12 Deployment Guide*, July, 2025
- *Veeam ONE Version 12 Monitoring Guide*, July, 2025
- *Veeam ONE Version 12 Reporting Guide*, July, 2025
- *Common Criteria Hardening Guide for v12*
- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 [APP_PP]

Assurance Continuity Maintenance Report:

Leidos submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on July 18, 2025 on behalf of Veeam Software. 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 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 Administrator's Guides, and the Impact Analysis Report (IAR). The ST and CC Admin Guide were updated.

Documentation updated:

Previous CC Evaluation Evidence	Evidence Change Summary
Security Target: *Veeam ONE v12 Security Target*, Version 1.6, 9 July 2023	**Maintained Security Target:** See references above. • Updated document version and date on cover page • Section 1.1 – Updated ST Version, ST Date, TOE Identification • Section 2.4 – Updated TOE documentation references • Appendix A – updated list of third-party libraries.
Design Documentation: See Security Target and Guidance	Minor changes required
Guidance Documentation: *Veeam ONE v12 Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, 9 July 2023	**Maintained Guidance Documentation:** See references above. • Updated document version and date on cover page • "Document Purpose and Scope" – updated TOE version number and TOE documentation references.
Supplementary Guidance Documentation Veeam ONE Version 12 Quick Start Guide, May, 2023 Veeam ONE Version 12 Deployment Guide, July, 2023 Veeam ONE Version 12 Monitoring Guide, July, 2023 Veeam ONE Version 12 Reporting Guide, July, 2023 Common Criteria Hardening Guide for v12	**Maintained Supplementary Guidance Documentation:** See references above. Quick Start Guide: • Updated document date on cover page. • Updated screenshots in section "Installing Veeam ONE". Deployment Guide: • Updated document date on cover page. • Added section "Connection to ServiceNow". • Reorganized information in section "Installing Veeam ONE". • Reorganized information in section "Upgrading to Veeam ONE 12". Monitoring Guide:

Previous CC Evaluation Evidence	**Evidence Change Summary**
	• Updated document date on cover page. • Added sub-sections “ServiceNow Integration”, “Syslog Integration”. • Reorganized information in section “Installing Veeam ONE Agents”. Reporting Guide: • Updated document date on cover page. • Added sections “Veeam Threat Center”, “Veeam Intelligence”. CC Hardening Guide: • No changes have been made to this document. These changes are considered minor, as they describe capabilities outside the scope of evaluation.
Lifecycle: None	No changes required.
Testing: Vendor regression testing	Vendor regression test results were produced and found consistent with the previous test results. Veeam performs extensive regression testing for every release including 12.3.
Vulnerability Assessment: Contained within IAR	**Maintained Vulnerability Assessment Documentation:** A new search was performed for public vulnerabilities from the time of the current validated release of the TOE (21 July 2023) to 17 July 2025. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were detected. The search was conducted against: • CVE (Common Vulnerabilities and Exposures) (https://cve.mitre.org/). The search covered the following: • “Veeam” – TOE vendor • “Veeam ONE” – TOE name

Previous CC Evaluation Evidence	Evidence Change Summary
	• Third Party Libraries identified in Appendix A of the Security Target.

Changes to the TOE:

The TOE changes consist of:

- Updates to Veeam ONE software from version 12 to version 12.3. The updates include new non-security relevant features and enhancements.

Major Changes

None.

Minor Changes

Category	Number of Changes	Applicability to New Firmware Versions
Feature Enhancements	15 (v12.1) 5 (v12.2) 7 (v12.3)	Version 12.1 introduced new features and enhancements in the following categories: • 5 enhanced functionality excluded from or not supported in the evaluated configuration • 10 enhanced product functionality without affecting evaluated security functionality Version 12.2 introduced new features and enhancements in the following categories: • 1 enhanced functionality excluded from or not supported in the evaluated configuration • 4 enhanced product functionality without affecting evaluated security functionality Version 12.3 introduced new features and enhancements in the following categories: • 2 enhanced functionality excluded from or not supported in the evaluated configuration • 5 enhanced functionality without affecting evaluated security functionality

Changes to the TOE Operational Environment:

Major Changes
None.

Minor Changes
None.

Equivalency:

The security functionality of Veeam ONE remains the same as the original evaluation. The hardware platform is unchanged from the previous maintained version.

NIST CAVP Certificates:

Veeam ONE v12.3 did not introduce any new cryptographic functionality; therefore, new CAVP certificates were not required.

Vulnerability Analysis:

An updated vulnerability analysis was performed on 17 July 2025 using the original search terms. No applicable vulnerabilities were found.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

The new features and other updates made to Veeam ONE from v12 through v12.1, v12.2, and v12.3 do not affect the security claims in the Veeam ONE v12 Security Target. These updates result in no changes to SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment and therefore constitute a minor change. The security target and the Common Criteria Evaluation Guidance Document are updated to reflect the firmware minor version update.

Regression testing was done and was considered adequate based on the scale and types of changes made. The laboratory also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, Veeam ONE v12.3 did not introduce any new cryptographic functionality; therefore, new CAVP certificates were not required. Therefore, CCEVS agrees that the original assurance is maintained for the product.