ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Veeam Backup & Replication v12.3.2

Veeam Backup & Replication v12.3.2

Maintenance Report Number: CCEVS-VR-VID11370-2025
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 Backup & Replication v12.3.2 Impact Analysis Report*, Version 1.0, 14 July 2025
- *Veeam Backup & Replication v12 Security Target*, Version 1.7, 8 July 2025
- *Veeam Backup and Replication v12 Common Criteria Evaluated Configuration Guide (CCECG),* Version 1.1, 8 July 2025
- *Veeam Backup & Replication Version 12 Quick Start Guide for VMware vSphere*, July 2025
- *Veeam Backup & Replication Version 12 User Guide for VMware vSphere*, July 2025
- *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 Backup & Replication v12 Security Target*, Version 1.6, 9 July 2023	**Maintained Security Target:** See references above. • Updated document version and date on cover page • 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 Backup & Replication 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 Backup & Replication Version 12 Quick Start Guide for VMware vSphere*, February, 2023 *Veeam Backup & Replication Version 12 User Guide for VMware vSphere*, July, 2023	**Maintained Supplementary Guidance Documentation:** See references above. Quick Start Guide: • Updated document date on cover page. • New section "Exporting Disks". User Guide: • Updated document date on cover page. • Reorganized some information in section "Planning and Preparation". • Added information on new/enhanced features: Malware Detection; Security & Compliance Analyzer. • Reorganized information in sections "Deployment" and "Getting Started with Veeam Backup & Replication" • Reorganized installation and configuration guidance. • Added section "Unstructured Data

Previous CC Evaluation Evidence	Evidence Change Summary
	Backup” 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 12.3.2.
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 15 July 2025. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were detected. Any outstanding CVEs discovered in versions prior to 12.3.2 have been addressed. The search was conducted against: • CVE (Common Vulnerabilities and Exposures) (https://cve.mitre.org/). The search covered the following: • “Veeam” – TOE vendor • “Backup and replication” – TOE name • Third Party Libraries identified in Appendix A of the Security Target.

Changes to the TOE:

The TOE changes consist of:

- Updates to Veeam Backup & Replication software from version 12 to version 12.3.2. The updates include new non-security relevant features and enhancements, and bug fixes.

Major Changes

None.

Minor Changes

Category	Number of Changes	Applicability to New Firmware Versions
Feature Enhancements	53 (v12.1) 30 (v12.2) 35 (v12.3) 14 (v12.3.1)	Version 12.1 introduced new features and enhancements in the following categories: • 17 enhanced functionality excluded from or not supported in the evaluated configuration • 36 enhanced product functionality without affecting evaluated security functionality Version 12.2 introduced new features and enhancements in the following categories: • 17 enhanced functionality excluded from or not supported in the evaluated configuration • 13 enhanced product functionality without affecting evaluated security functionality Version 12.3 introduced new features and enhancements in the following categories: • 22 enhanced functionality excluded from or not supported in the evaluated configuration • 13 enhanced functionality without affecting evaluated security functionality Version 12.3.1 introduced new features and enhancements in the following categories: • 12 enhanced functionality excluded from or not supported in the evaluated configuration • 2 enhanced product functionality without affecting evaluated security functionality

Bug Fixes	9 (v12.3.1) 7 (v12.3.2)	Version 12.3.1 also included 9 bug fixes in the following categories: • 6 fixed functionality excluded from or not supported in the evaluated configuration • 3 fixed product functionality without affecting evaluated security functionality Version 12.3.2 also included 7 bug fixes in the following categories: • 4 fixed functionality excluded from or not supported in the evaluated configuration • 3 fixed product functionality without affecting evaluated security functionality Examples of behavior corrections were: Fixed an issue where Microsoft's deprecation of Basic SKU Public IP Addresses prevents the creation of Azure appliances; fixed an issue where when deleting backups from disk, the backup console required a decryption password to be provided for encrypted backups; fixed an issue where marking malware events as clean failed with a conversion error when the Microsoft SQL Server hosting the configuration database used the German (DE) locale; fixed an issue where in rare circumstances, application-aware image processing could hang during the guest components installation. None of the bug fixes affected the security functionality and none of the changes resulted in changes to the ST or the guidance documentation other than updates to reflect the firmware minor version update. These changes were either unrelated to SFR testing or were not visible at the level of testing performed for the SFRs. Thus, the original testing still holds, and any fix testing was covered by vendor non-evaluation regression and checkout testing. CVEs related to VBR affect earlier versions than v12.3.2 and have been addressed.

Changes to the TOE Operational Environment:

Major Changes
None.

Minor Changes
None.

Equivalency:

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

NIST CAVP Certificates:

Veeam Backup & Recovery v12.3.2 did not introduce any new cryptographic functionality; therefore new CAVP certificates were not required.

Vulnerability Analysis:

An updated vulnerability analysis was performed on 15 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 Backup & Replication from v12 through v12.1, v12.2, v12.3, v12.3.1, and v12.3.2 do not affect the security claims in the Veeam Backup & Replication 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 Backup & Recovery v12.3.2 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.