National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Veeam Backup & Replication v12

Report Number: CCEVS-VR-VID11370-2023
Dated: August 18, 2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Sheldon Durrant

Lisa Mitchell

Linda Morrison

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Veeam Backup & Replication v12 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])

The TOE is Veeam Backup & Replication v12.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile, and when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([6]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Veeam Backup & Replication v12, evaluated on Microsoft Windows Server 2019.
Security Target	Veeam Backup & Replication v12 Security Target, Version 1.6, 9 July 2023
Sponsor & Developer	Veeam Software Corporation 8800 Lyra Drive Suite 350 Columbus, OH 43240
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*Protection Profile for Application Software*, Version 1.4, 7 October 2021
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Evaluation Personnel	Anthony Apted Kofi Owusu Pascal Patin
Validation Personnel	Sheldon Durrant Lisa Mitchell Linda Morrison

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE is a software application. In its evaluated configuration, it is installed on an instance of Microsoft Windows Server 2019 executing on an x86-64 processor.

The following figure provides a diagrammatic depiction of the TOE architecture.

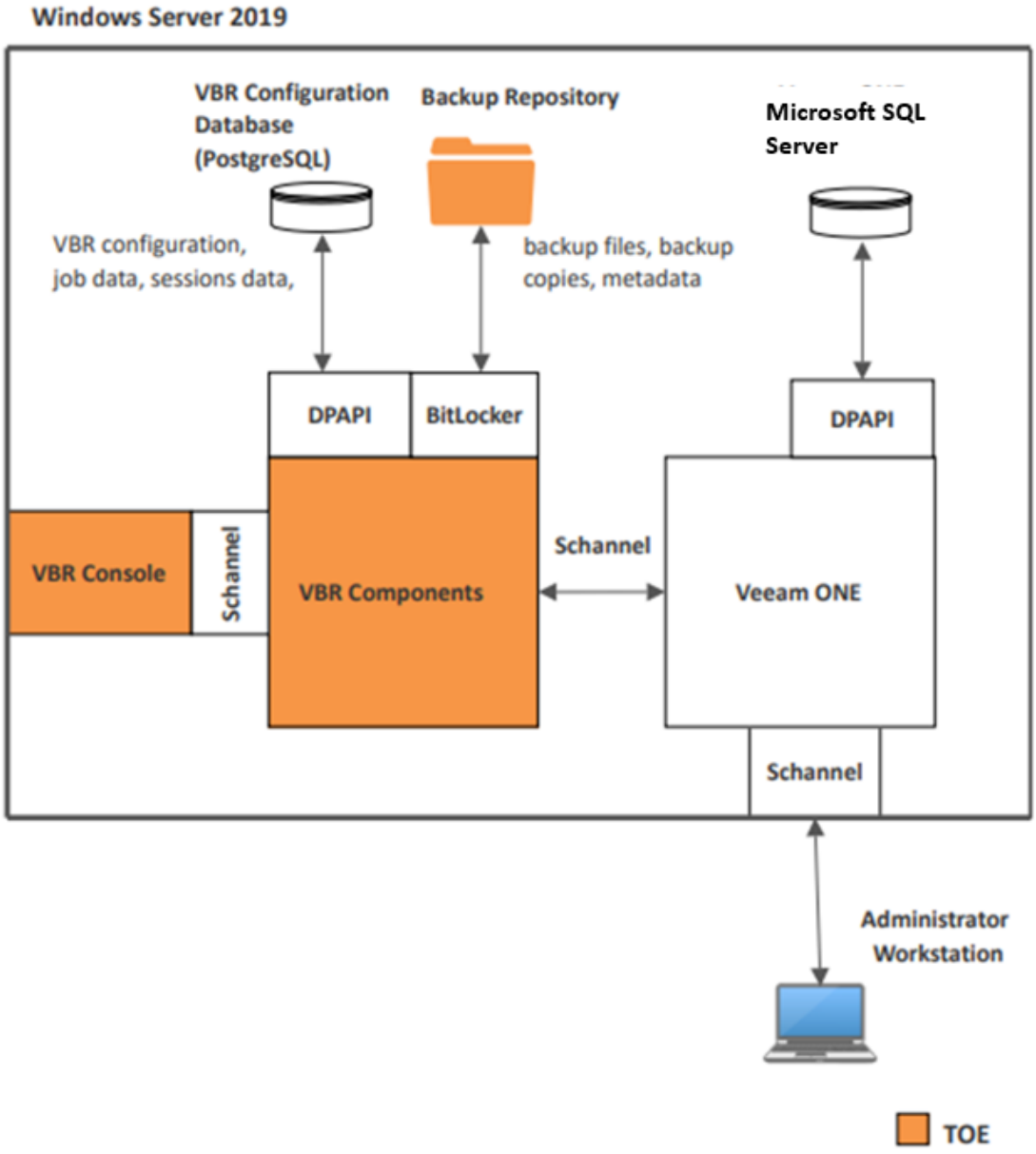


Figure 1: Veeam Backup & Replication Architecture

The TOE consists of the following components:

- **Backup Server Component**—performs main management operations, coordinates backup, replication and restore tasks, controls job scheduling and resource allocation.

- **Backup Proxy**—sits between the Backup Server Component and other components of the backup infrastructure. While the Backup Server Component administers tasks, the Backup Proxy processes jobs and delivers backup traffic. The Backup Proxy tasks include the following:
  - Retrieving VM data from the production storage
  - Compressing
  - Deduplicating
  - Encryption
  - Sending data to the Backup Repository (for a backup job) or another Backup Proxy (for a replication job)
- **VBR Console**—provides the application user interface and allows user access to the application functionality. In the evaluated configuration, the VBR Console is installed on the same host as the other VBR components. A user must have local Administrator permissions to invoke the VBR Console and must have SeBackupPrivilege and SeRestorePrivilege to connect to the Backup Server Component.
- **Backup Repository**—location where backup files, backup copies and metadata of replicated VMs are stored. During installation, VBR checks volumes of the machine on which VBR is installed and identifies a volume with the greatest amount of free disk space. On this volume, VBR creates the Backup folder that is used as the default Backup Repository.

The TOE has the following minimum requirements for the Microsoft Windows Server 2019 platform on which it is installed:

Item	Minimum Requirements
CPU	x86-64 processor (minimum 4 cores recommended)
Memory	4 GB RAM plus 500 MB RAM for each concurrent job
Disk Space	5 GB for product installation and 4.5 GB for Microsoft .NET Framework 4.7.2 installation. 10 GB per 100 VM for guest file system catalog folder (persistent data)
Additional Software	PostgreSQL 15.1 System Center Virtual Machine Manager 2012 SP1 to 2019 Admin UI (optional, to register SCVMM server with Backup & Replication infrastructure) Microsoft .NET Framework 4.7.2 (included in the setup) Windows Installer 4.5 (included in the setup) Microsoft Windows PowerShell 5.1 (included in the setup)

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Cryptographic Support

The TOE invokes platform-provided cryptography to protect data at rest. The TOE invokes the Data Protection API (DPAPI) to store configuration data, job data, and session data and relies on BitLocker to protect backup files and metadata stored in non-volatile memory.

4.2 User Data Protection

The TOE accesses the minimum amount of Windows Server hardware and data in order to perform its function. The TOE stores database connectivity information in the Windows Registry and stores other TOE configuration information in the PostgreSQL database.

4.3 Security Management

Both the TOE binary components themselves and the configuration settings they use are stored in locations recommended for Microsoft Windows Server.

The TOE includes a console user interface (UI). Users must login to Windows and have permissions to access the UI in order to access the TOE.

Administrators use the console UI to configure the backup tasks to be performed by the TOE.

4.4 Privacy

The TOE does not process any personally identifiable information (PII).

4.5 Protection of the TSF

The TOE enforces various mechanisms to prevent itself from being used as an attack vector to its Windows platform. The TOE implements address space layout randomization (ASLR), does not allocate any memory with both write and execute permissions, does not write user-modifiable files to directories that contain executable files, is compiled using stack overflow protection, and is compatible with the Windows Defender security features of its host platform.

The TOE contains libraries and invokes system APIs that are well known and explicitly identified.

The TOE has a mechanism to display its current software version. The TOE can be used to determine if software updates for it are available. If so, an administrator uses out of band mechanisms to acquire, validate, and install the update securely.

The TOE developer provides a secure mechanism for receiving reports of security flaws. Product vulnerabilities are tracked and addressed, and software updates are securely distributed to customers in a timely manner.

4.6 Trusted Path/Channels

The TOE does not transmit any sensitive data between itself and another trusted IT product.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP_APP_V1.4 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following document:
  - *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Veeam Backup & Replication v12 Security Target*, Version 1.6, 9 July 2023 ([6]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Veeam Backup & Replication Version 12 User Guide for VMware vSphere*, July 2023 ([7])
- *Veeam Backup & Replication Version 12 Quick Start Guide for VMware vSphere*, February 2023 ([8])
- *Veeam Backup and Replication v12 Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, July 9, 2023 ([9]).

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Veeam Backup and Replication (VBR) 12 Common Criteria Test Report and Procedures For Application Software Version 1.4*, Version 1.0, 21 July 2023 ([12]).

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Veeam Backup & Replication*, Version 1.0, 14 August 2023 ([11])

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

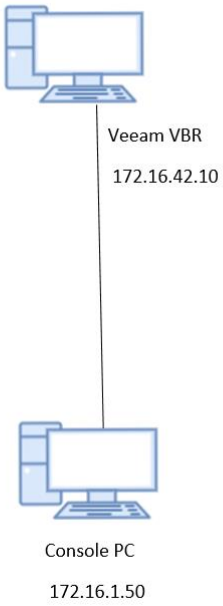
The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the following specification:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021.

The evaluation team devised a test plan based on the test activities specified in the PP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report listed above.

The TOE was tested at Leidos's Columbia, MD location from May 2023 to August 2023. The procedures and results of this testing are available in the test report referenced above.

The following figure identifies the devices used for testing the TOE and describes the test configuration.



Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *Protection Profile for Application Software* were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is Veeam Backup & Replication v12, evaluated on Microsoft Windows Server 2019.

8.2 Excluded Functionality

The scope of the evaluation excludes the following:

- Off-site data protection—only on-site data protection is supported. This excludes Veeam Cloud Connect from the evaluated configuration.
- Veeam Agent management—VBR uses backup agents installed on the target platform to back up physical machines running Windows, Linux, Unix or macOS operating systems
- Network-Attached Storage (NAS)—VBR supports backup up and restore of content of various NAS file shares. The scope of evaluation excludes NAS backup
- Tape Device Support—Veeam provides native tape support that is fully integrated into VBR. .
- Remote VBR Console—the evaluated configuration excludes support for remote instances of the VBR Console
- Object Storage Repositories—repositories intended for long-term data storage. It can be based on either a cloud solution or an S3 compatible storage solution. Object Storage Repositories and virtual machine backup are not supported in the evaluated configuration.

8.3 VBR Tools Excluded from the Evaluated Configuration

The VBR application includes the following utilities that enable an Administrator to perform advanced administration tasks. The following tools/utilities are excluded from the evaluated configuration.

- **Extract.exe Utility**: The VBR application includes an extract utility that can be used to recover machines from backup files. The extract utility does not require any interaction with VBR and can be used as an independent tool on Linux and Microsoft Windows machines.
- **Veeam.Backup.DBConfig.exe Utility**: VBR includes the Veeam.Backup.DBConfig.exe utility that allows an Administrator to manage connections settings for VBR and/or Veeam Backup Enterprise Manager configuration database.
- **Veeam Backup Validator**: Veeam Backup Validator is a utility that verifies the integrity of a backup file without extracting VM data. Veeam Backup Validator is a command-prompt CRC check utility that tests a backup at the file level. An Administrator may need this utility to check whether backup files were damaged.
- **Veeam Backup Configuration Tool**: The VBR application includes Veeam.Backup.Configuration.Tool.exe that enables an Administrator to manage BCO files. BCO files are backup files that contain backups of configuration databases.
- **Veeam Backup PowerShell Module** is an extension for Microsoft Windows PowerShell that adds a set of cmdlets to allow users to perform backup, replication and recovery tasks through the command-line interface of PowerShell or run custom scripts to fully automate operation of Veeam Backup & Replication.

8.4 VBR Parameters Supported in the Evaluated Configuration

- Windows Session Authentication is required in the evaluated configuration.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Veeam Backup & Replication v12 ([10]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 ([5]).

The evaluation determined the TOE satisfies the conformance claims made in the Veeam Backup & Replication v12 Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the PP listed above.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PP, and security function descriptions that satisfy the requirements.

9.2 The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA evaluation activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the National Vulnerability Database (https://nvd.nist.gov/).

The evaluation team performed searches on 21 July 2023, using the following search terms:

- “veeam”
- “backup and replication”
- The identity of each of the third-party libraries listed in Appendix A, Table 9, of the ST.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. In addition, the evaluation team's testing demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The validation team notes that the evaluated configuration is based on the TOE being deployed on a single instance of Microsoft Windows Server 2019. Communication with Veeam ONE v12, installed on the same server, is over Schannel, so secure communications is not included in the evaluated configuration. As noted in the Security Target, only the ability to backup and restore the local PostgreSQL configuration database is within scope of the evaluation.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Security Target

The ST for this product's evaluation is *Veeam Backup & Replication v12 Security Target*, Version 1.6, 9 July 2023 ([6]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VBR	Veeam Backup & Replication
VR	Validation Report

13 Bibliography

The validation team used the following documents to produce this VR:

[1] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements*, Version 3.1, Revision 5, April 2017.

[4] *Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, April 2017.

[5] *Protection Profile for Application Software*, Version 1.4, 07 October 2021.

[6] *Veeam Backup & Replication v12 Security Target*, Version 1.6, 9 July 2023.

[7] *Veeam Backup & Replication Version 12 User Guide for VMware vSphere*, July 2023

[8] *Veeam Backup & Replication Version 12 Quick Start Guide for VMware vSphere*, February 2023

[9] *Veeam Backup and Replication v12 Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, 9 July 2023.

[10] *Evaluation Technical Report for Veeam Backup & Replication v12*, Version 1.0, 14 August 2023.

[11] *Assurance Activities Report for Veeam Backup & Replication v12*, Version 1.0, 14 August 2023.

[12] *Veeam Backup and Replication (VBR) 12 Common Criteria Test Report and Procedures For Application Software Version 1.4*, Version 1.0, 21 July 2023.

[13] *Veeam Backup & Replication v12 Vulnerability Assessment*, Version 1.1, 14 August 2023.