Veeam Backup & Replication v12

Security Target

Version 1.6
9 July 2023

Veeam Software
8800 Lyra Drive Suite 350
Columbus, Ohio 43240

Prepared by:
Leidos Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, Maryland 21046

Contents

List of Figures and Tables

1. Security Target Introduction

The Security Target (ST) contains the following additional sections:

- Product and TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)
- TOE Usage of Third-Party Libraries (Appendix A)

1.1 Security Target, Target of Evaluation, and Common Criteria Identification

ST Title: Veeam Backup & Replication v12 Security Target

ST Version: 1.6

ST Date: 9 July 2023

Target of Evaluation (TOE) Identification: Veeam Backup & Replication v12

TOE Developer: Veeam Software, Inc.

Evaluation Sponsor: Veeam Software, Inc.

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes claim exact conformance to the following CC specifications:

- *Protection Profile for Application Software,* Version 1.4, 7 October 2021 (PP_APP_v1.4) with the following optional and selection based SFRs:
  - FPT_TUD_EXT.2

The following table identifies the NIAP Technical Decisions that apply to the TOE and have been accounted for in the ST development and the conduct of the evaluation or were determined to be non-applicable.

Table 1: Technical Decisions

TD #	TD Title	Applicability to Evaluation
0624	Addition of DataStore for Storing and Setting Configuration Options	Applicable to FMT_MEC_EXT.1 but the TD only applies to testing activities.
0628	Addition of Container Image to Package Format	Applicable to FPT_TUD_EXT.2

TD #	TD Title	Applicability to Evaluation
0650	Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4.	Not applicable because the ST does not implement a VPN.
0664	Testing activity for FPT_TUD_EXT.2.2.	Applicable because the TOE claims FPT_TUD_EXT.2.2 but the TD only applies to testing activities.
0669	FIA_X509_EXT.1 Test 4 Interpretation.	Not applicable because the ST does not claim FIA_X509_EXT.1.
0717	Format changes for PP_APP_V1.4.	Applicable because the TD archives two TDs.
0719	ECD for PP APP V1.3 and 1.4	Applicable because the TD defines extended components.
0736	Number of elements for iterations of FCS_HTTPS_EXT.1	The TD is not applicable. The ST does not include FCS_HTTPS_EXT.1/Server.
0743	FTP_DIT_EXT.1.1 Selection exclusivity	Applicable because the ST claims conformance to the App PP and the ST includes FTP_DIT_EXT.1.
0756	Update for platform-provided full disk encryption	The TD is applicable to the evaluation. The TOE implements FDP_DAR_EXT.1 and platform provided cryptography. The TD affects the Test evaluation activity.

- *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.
  - Part 3 Extended

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. An iterated SFR is indicated by a slash followed by a descriptor for the purpose of the iteration. For example, FCS_HTTPS_EXT.1/Client indicates that the FCS_HTTPS_EXT.1 requirement applies specifically to HTTPS client functionality.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using italics and are surrounded by brackets (e.g., [*assignment item*]). Note that an assignment within a selection would be identified in both italics and underline, with the brackets themselves underlined since they are explicitly part of the selection text, unlike the

brackets around the selection itself (e.g., [selection item, [*assignment item inside selection*]]).

- Selection: allows the specification of one or more elements from a list. Selections are indicated using underlines and are surrounded by brackets (e.g., [selection item]). Note that a selection within a selection would be identified underlined with the brackets themselves underlined since they are explicitly part of the selection text, unlike the brackets around the selection itself (e.g., [selection item, [selection inside selection]]).
- Refinement: allows technical changes to a requirement to make it more restrictive and allows non-technical changes to grammar and formatting. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that minor grammatical changes that do not involve the addition or removal of entire words (e.g., for consistency of quantity such as changing "meets" to "meet") do not have formatting applied.

- The ST does not show operations that have been completed by the PP authors.

1.3.1 Acronyms and Abbreviations

Table 2: Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
.VBK	File extension for a full backup of the entire VM.
.VBM	File extension for a metadata file that contains information on a backup job.
.VIB	File extension for an incremental backup file.
.VRB	File extension for an incremental backup file.
API	Application Programming Interface
AES	Advanced Encryption Standard
ASLR	Address Space Layout Randomization
AWS	Amazon Web Services
BCO	Backup Configuration
CAVP	Cryptographic Algorithm Validation Program
CDP	Continuous Data Protection
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CLR	Common Language Runtime
CRC	Cyclic Redundancy Check
DRBG	Deterministic Random Bit Generator
DPAPI	Data Protection API
GB	Gigabyte
NAS	Network-Attached Storage

Acronym/ Abbreviation	Definition
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
Schannel	Secure Channel
SCVMM	System Center Virtual Machine Manager
SFR	Security Functional Requirement
SMO	Server Management Objects
SP	Service Pack
ST	Security Target
SWID	Software Identification
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol
UI	User Interface
VBR	Veeam Backup & Replication
VM	Virtual Machines

1.3.2 Terminology

Table 3: Definitions

Term	Definition
BCO files	Backup files that contain backups of configuration databases. Veeam creates these files when it performs a configuration backup.
BitLocker	BitLocker is an encryption feature included with Microsoft Windows. It protects data by providing encryption for entire volumes. It uses AES CBC or XTS w/ a 128-bit or 256-bit key. In this application it is used to encrypt backup data.

Term	Definition
DPAPI	DPAPI is an API provided by .NET third party library.
Deduplicating	The elimination of duplicate or redundant information.
Deduplicating Storage Appliance	Data deduplication hardware is disk storage that eliminates redundant copies of data and retains one instance to be stored. Hardware-based deduplication products perform deduplication at the target rather than the source, or server.
Object Storage Repositories	Is a repository intended for long-term data storage. It can be based on either a cloud solution or an S3 compatible storage solution. Object Storage Repositories are not supported in the evaluated configuration.
Restore Point	A backup copy of files and settings that can be used to recover the system to an earlier point of time.
RPO	RPO defines a period during which a site may accept to lose data. It is the age of the latest backup that will be used for recovery in case of a failure.
RTO	RTO represents the amount of time from the beginning of an incident until all servicers are back online and available.
S3	S3 or Amazon Simple Storage Service is a service offered by Amazon that provides object storage through a web service interface.
VBR Console	The VBR Console is automatically installed on the Backup Server. Additionally, Administrators have the option of installing the VBR Console on remote machines.
Backup Server Component	The Backup Server Component performs main management operations, coordinates backup, replication and restore tasks, controls job scheduling and resource allocation.
Veeam Continuous Data Protection (CDP)	A technology that aids in protecting mission-critical VMware virtual machines when data loss for seconds or minutes is unacceptable. CDP also provides minimum recovery time objective (RTO) in case a disaster strikes because VM replicas are in a ready-to-start state.

2. Product and TOE Description

2.1 Product Overview

The Veeam Availability Suite™ is an application suite consisting of two components: Veeam Backup & Replication and Veeam ONE. Veeam Backup & Replication provides cloud, virtual and physical backup and recovery options as well as image-based virtual machine (VM) replication from a VM or backup. Veeam ONE provides real-time monitoring, reporting and intelligent tools for Veeam Backup & Replication, VMware vSphere, and Microsoft Hyper-V.

This Security Target defines the Target of Evaluation (TOE) as the Veeam Backup & Replication application component of the Veeam Availability Suite™. The TOE conforms to the *Protection Profile for Application Software,* Version 1.4, 7 October 2021 ([App PP]). As such, the security-relevant functionality of the product is limited to the requirements claimed in this ST.

2.2 TOE Overview

Veeam Backup & Replication (VBR) is a software application that provides backup and recovery for a wide range of systems and clouds including:

- Physical: Windows, Linux, MacOS, and NAS.
- Virtual: VMware vSphere, Microsoft Hyper-V, and Nutanix AHV.
- Cloud: AWS EC2 instance, Microsoft Azure, Office 365, IBM Cloud, and Google Cloud.

VBR backup is performed by VBR by retrieving VM data from the source storage, compressing it, and deduplicating it. VBR then writes data to the Backup Repository in Veeam proprietary format. Administrators have the option to perform the following:

- Full back up file (.VBK) that contains a copy of the entire VM.
- Incremental backup file (.VIB or .VRB) that contains only those data blocks that have changed since the last backup job.
- Metadata file (.VBM) that contains information on the backup job, VMs in the backup, number of structures of backup files, and restore points.

VBR supports a Backup Copy function that enables an Administrator to create several instances of the same backup data in different locations.

Restore performs restore from backup files to the original or a new location. Veeam VBR offers recovery options for various disaster recovery scenarios including Instant Recovery, image-level restore, file-level restore, and restore of application items.

Replication is when VBR creates the exact copy of the VM in the native VMware vSphere format on a spare ESXi host and keeps this copy synchronized with the original VM. Replication provides the best recovery time objective (RTO) values and is recommended for VMs running critical applications. VBR supports both onsite replication and offsite replication.

VBR includes Continuous Data Protection (CDP), a replication technology that helps protect mission critical VMs and reach recovery point objective (RPO) up to seconds. CDP also provides minimum recovery time objective (RTO) in case a disaster strikes because VM replicas are in a ready-to-start state.

2.3 TOE Architecture

The Veeam Backup & Replication infrastructure consists of the following core components.

- **Backup Server Component**: performs main management operations, coordinates backup, replication and restore tasks, controls job scheduling and resource allocation.
- **Backup Proxy**: a component that sits between the Backup Server 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**: A VBR component that provides the application user interface and allows user access to the application functionality.
- **Backup Repository**: A backup repository 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.

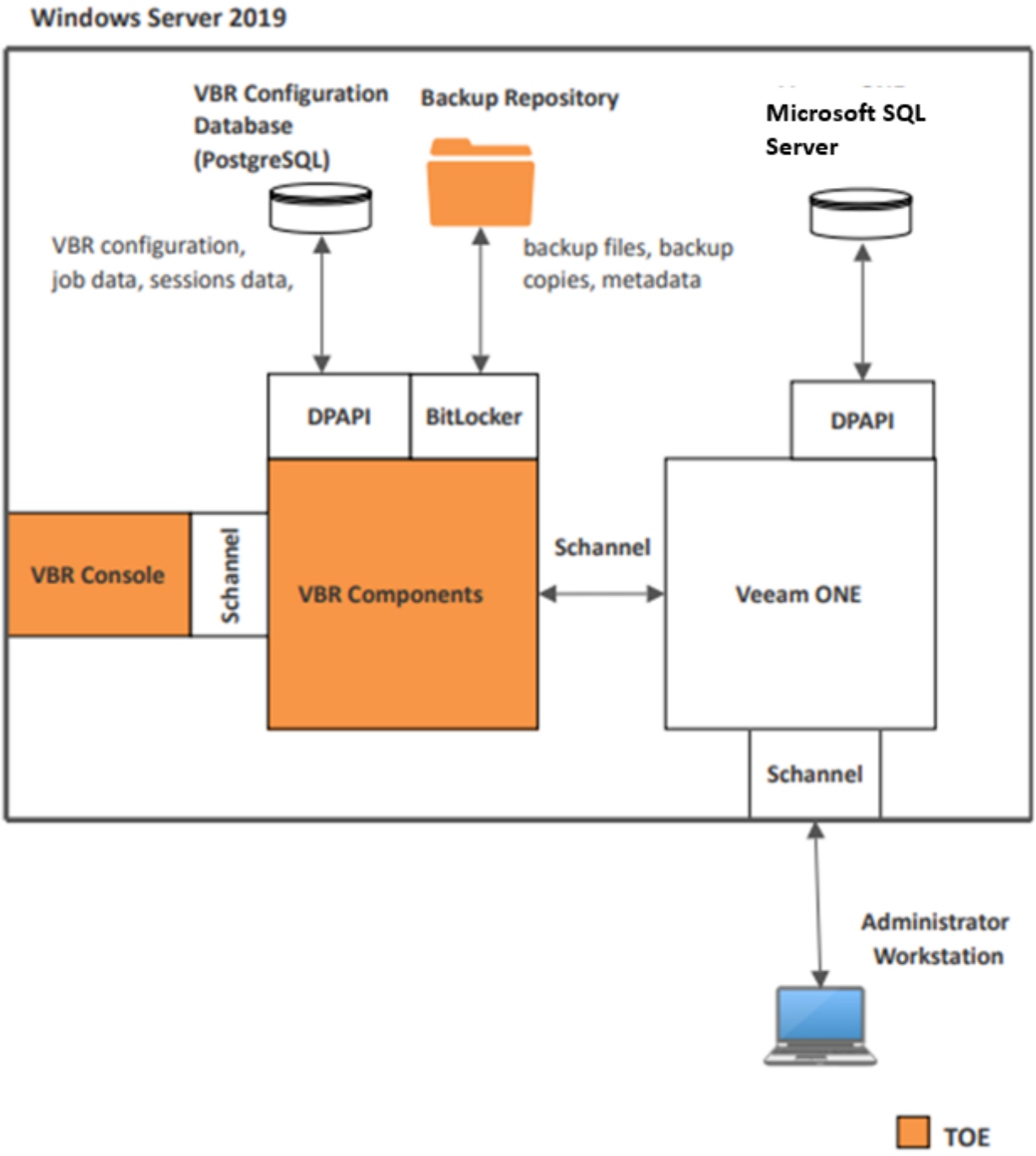
VBR's supporting environment includes the following systems.

- **VBR Configuration Database:** stores data about the backup infrastructure, jobs, sessions and other configuration data. The database instance can be located on a PostgreSQL Server installed either locally (on the same machine where the backup server is running) or remotely.
- **Infrastructure servers and hosts**: Servers that are source and target for backup, replication, and other activities.
- **Backup Server**: A host machine or virtual machine on which Veeam Backup & Replication is installed.

The VBR Console is invoked locally. The Administrator must have local Administrator permissions to invoke the VBR Console. Upon invocation of the VBR Console, the Administrator is prompted for which VBR the Administrator would like to connect to. The default host is the local host. The Administrator must have SeBackupPrivilege and SeRestorePrivilege to connect to the Backup Server.

2.3.1 Physical Boundary

Figure 1: VBR TOE Physical Boundary



The Veeam Backup and Replication (VBR) TOE is the set of Veeam applications and services which are installed on a Windows-based machine. The figure above depicts the TOE components in relationship to the platform provided functionality.

The VBR Components included in the TOE boundary (and described in section 2.3 TOE Architecture above) are:

- **Backup Server Component**
- **Backup Proxy**
- **VBR Console**

VBR supports two managed repositories. The **Backup Repository**, which stores backup files, backup copies and metadata of replicated VMs and the **VBR Configuration Database**, implemented using PostgreSQL, used to store data about the backup infrastructure, jobs, sessions and other configuration data. The **Backup Repository** is inside the TOE boundary. The **VBR Configuration Database** is outside the TOE boundary.

The TOE uses platform provided Windows Microsoft Secure Channel (Schannel) to provide communication between the VBR Console and the VBR Components. The connection from the console to VBR Components is to localhost, so the communication stack is not reached. Platform provided Windows Data Protection Application Programming Interface (DPAPI) is used to store backup infrastructure information, job data, session data and other configuration data in the VBR Configuration Database. Backup files and metadata are stored in the Backup Repository using the platform-provided BitLocker.

2.3.1.1 Evaluated Configuration

For this evaluation, the TOE will be deployed on a single instance that provides the full functionality required to evaluate all security functions. In addition, only the ability to backup and restore the configuration database is within scope of the evaluation.

The TOE is installed on a single Windows Server with the following minimum requirements.

Table 4: Windows Server Minimum Requirements for VBR Backup Server

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)
OS	Only 64-bit versions of the following operating system: • Microsoft Windows Server 2019

Item	Minimum Requirements
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)

The TOE was installed on a platform with Windows Server 2019 Standard edition. The platform processor was the Intel Xeon Gold 6126 CPU @ 2.60 GHz. The processor is included in the Skylake microarchitecture.

The TOE in the evaluated configuration performs a backup and restore of the configuration database. Therefore, there are no operational environmental requirements of the evaluated configuration.

2.3.1.2 Functionality Excluded from the Evaluated Configuration

The following components/functionality/configurations/tools are excluded from the evaluated configuration.

Infrastructure

- **Off-site data** protection is excluded; only on-site data protection is supported. This excludes Veeam Cloud Connect from the evaluated configuration.
- **Veeam Agent Management**: To back up physical machines running Windows, Linux, Unix or macOS operating systems, VBR uses backup agents installed on each computer. VBR operates as a centralized control center for deploying and managing:
  - Veeam Agent for Microsoft Windows
  - Veeam Agent for Linux
  - Veeam Agent for IBM AIX
  - Veeam Agent for Oracle Solaris and
  - Veeam Agent for Mac
- **Network-Attached Storage (NAS):** VBR supports backup up and restore of content of various NAS file shares. NAS backup is excluded from the evaluated configuration.
- **Tape Device Support:** Veeam provides native tape support that is fully integrated into VBR. Long-term archiving and compliance are listed as primary reasons for using tape.
- **Remote VBR Console:** Support for remote instances of the VBR Console are not included in the evaluated configuration.
- **Object Storage Repositories:** Is a repository 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.

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.

2.3.1.3 VBR Parameters Supported in the Evaluated Configuration

- Windows Session Authentication is required in the evaluated configuration.

2.3.2 Logical Boundary

This section summarizes the security functions provided by the TOE:

- Cryptographic Support
- User Data Protection
- Security Management
- Privacy
- Protection of the TSF
- Trusted path/Channels

2.3.2.1 Cryptographic Support

The TOE invokes platform-provided cryptography to protect data at rest.

For data at rest, the platform provided DPAPI stores configuration data, job data and session data, and the platform provided BitLocker is used to protect backup files and metadata stored in non-volatile memory.

2.3.2.2 User Data Protection

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

2.3.2.3 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 UI. Users must login to Windows and have permissions to access the UI in order to access the TOE.

The console UI is used to configure the backup tasks to be performed by the TOE.

2.3.2.4 Privacy

The TOE does not handle personally identifiable information (PII) of any individuals.

2.3.2.5 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 securely acquire, validate, and install the update.

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.

2.3.2.6 Trusted Path/Channels

The TOE does not support any network interfaces and therefore, does not provide protection of data in transit.

2.4 TOE Documentation

Veeam provides the following product documentation in support of the installation and secure use of the TOE.

- Veeam Backup & Replication Version 12 User Guide for VMware vSphere, July, 2023
- Veeam Backup & Replication Version 12 Quick Start Guide for VMware vSphere, February, 2023

- Veeam Backup and Replication v12 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, July 9, 2023

3. Security Problem Definition

This ST includes by reference the Security Problem Definition, composed of threats and assumptions, from the App PP. The Common Criteria also provides for organizational security policies to be part of a security problem definition, but no such policies are defined in the App PP.

In general, the threat model of the App PP is designed to protect against the following:

- Disclosure of sensitive data at rest or in transit that the user has a reasonable expectation of security for.
- Excessive or poorly-implemented interfaces with the underlying platform that allow an application to be used as an intrusion point to a system.

It is applicable because the TOE is a collection of executable binaries that an attacker could attempt to use to compromise the underlying OS platform if it was designed in such a manner that this exploitation was possible.

4. Security Objectives

Like the Security Problem Definition, this ST includes by reference the security objectives defined in the App PP. This includes security objectives for the TOE (used to mitigate threats) and for its operational environment (used to satisfy assumptions).

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the following Protection Profile (PP):

- *Protection Profile for Application Software*, Version 1.4, October 07, 2021 (App PP)

As a result, any selection, assignment, or refinement operations already performed by that PP on the claimed SFRs are not identified here (i.e., they are not formatted in accordance with the conventions specified in section 1.3 of this ST). Formatting conventions are only applied on SFR text that was chosen at the ST author's discretion.

5.1 Extended Requirements

All the extended requirements in this ST have been drawn from the App PP. The App PP defines the following extended SAR and extended SFRs; since they have not been redefined in this ST, the App PP should be consulted for more information regarding these extensions to CC Parts 2 and 3.

Extended SARs:

- ALC_TSU_EXT.1 Timely Security Updates

Extended SFRs:

- FCS_CKM_EXT.1 Cryptographic Key Generation Services
- FCS_RBG_EXT.1 Random Bit Generation
- FCS_STO_EXT.1 Storage of Credentials
- FDP_DAR_EXT.1 Encryption of Sensitive Application Data
- FDP_DEC_EXT.1 Access to Platform Recourses
- FDP_NET_EXT.1 Network Communications
- FMT_CFG_EXT.1 Secure by Default Configuration
- FMT_MEC_EXT.1 Supported Configuration Mechanism
- FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information
- FPT_AEX_EXT.1 Anti-Exploitation Capabilities
- FPT_API_EXT.1 User of Supported Services and APIs
- FPT_IDV_EXT.1 Software Identification and Versions
- FPT_LIB_EXT.1 Use of Third Party Libraries
- FPT_TUD_EXT.1 Integrity for Installation and Update
- FPT_TUD_EXT.2 Integrity for Installation and Update
- FTP_DIT_EXT.1 Protection of Data in Transit

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Table 5: TOE Security Functional Components

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_CKM_EXT.1 Cryptographic Key Generation Services
	FCS_RBG_EXT.1 Random Bit Generation Services
	FCS_STO_EXT.1 Storage of Credentials
FDP: User Data Protection	FDP_DAR_EXT.1 Encryption of Sensitive Application Data
	FDP_DEC_EXT.1 Access to Platform Resources
	FDP_NET_EXT.1 Network Communications
FMT: Security Management	FMT_CFG_EXT.1 Secure by Default Configuration
	FMT_MEC_EXT.1 Supported Configuration Mechanism
	FMT_SMF.1 Specification of Management Functions
FPR: Privacy	FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information
FPT: Protection of the TSF	FPT_AEX_EXT.1 Anti-Exploitation Capabilities
	FPT_API_EXT.1 Use of Supported Services and APIs
	FPT_IDV_EXT.1 Software Identification and Versions
	FPT_LIB_EXT.1 Use of Third Party Libraries
	FPT_TUD_EXT.1 Integrity for Installation and Update
	FPT_TUD_EXT.2 Integrity for Installation and
FTP: Trusted Path/Channels	FTP_DIT_EXT.1 Protection of Data in Transit

5.2.1 Cryptographic Support (FCS)

5.2.1.1 FCS_CKM.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1[1] The application shall [

- generate no asymmetric cryptographic keys,

].

[1] Modified per TD0717.

5.2.1.2 FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [

- use no DRBG functionality,

] for its cryptographic operations.

5.2.1.3 FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [

- not store any credentials

] to non-volatile memory.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [

- leverage platform-provided functionality to encrypt sensitive data,

] in non-volatile memory.

5.2.2.2 FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [

- no hardware resources,

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- *[backup data, job data and session data (event logs)]*

].

5.2.2.3 FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- [no network communication]

].

5.2.3 Security Management (FMT)

5.2.3.1 FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

5.2.3.2 FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1 The application shall [invoke the mechanisms recommended by the platform vendor for storing and setting configuration options].

5.2.3.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [

- *[backup and restore the configuration database]*

].

5.2.4 Privacy (FPR)

5.2.4.1 FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [

- not transmit PII over a network

] .

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Anti-Exploitation Capabilities (FPT_AEX_EXT.1)

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [*no exceptions*].

FPT_AEX_EXT.1.2 The application shall [

- not allocate any memory region with both write and execute permissions

].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

5.2.5.2 FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

5.2.5.3 FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with [[*a Major, Minor, and Build Number*]].

5.2.5.4 FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [*the third-party libraries identified in Appendix A*].

5.2.5.5 FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [provide the ability] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed [as an additional software package to the platform OS].

5.2.5.6 FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1[2] The application shall be distributed using [the format of the platform-supported package manager].

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.2.6 Trusted Path/Channels (FTP)

5.2.6.1 FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1[3] The application shall [

- not transmit any [data]

] between itself and another trusted IT product.

[2] This SFR is modified by TD0628.

[3] This SFR is modified by TD0743.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference to the App PP.

Table 6: Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance Documentation	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative Procedures
ALC: Life-cycle Support	ALC_CMC.1 Labeling of the TOE
	ALC_CMS.1 TOE CM coverage
	ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_IND.1 Independent Testing – Conformance
AVA: Vulnerability Assessment	AVA_VAN.1 Vulnerability Survey

The evaluation activities specified in the App PP apply to the entire TOE evaluation, including any changes made to them by subsequent NIAP Technical Decisions as summarized in section 1.2 above.

6. TOE Summary Specification

This chapter describes the following security functions:

- Timely Security Updates
- Cryptographic Support
- User Data Protection
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels

6.1 Timely Security Updates

Users may submit security issues to Veeam via https://www.veeam.com/vulnerability-disclosure.html?ad=in-text-link. Availability of updates is announced via email sent to customers as well as via the Veeam website. Updates are provided within 60 days of public disclosure of vulnerabilities, including those for third-party components.

6.2 Cryptographic Support

The TOE invokes platform-provided cryptographic functionality for the following purposes:

- Encrypt VBR configuration data, job data, and session data in the VBR Configuration Database (PostgreSQL) using platform-provided DPAPI.
- Encrypt backup files, backup copies, and file metadata in the VBR Backup Repository using platform-provided BitLocker.
- Note that VBR Console to VBR is via Schannel but because the connection is localhost, the calling program does not reach the communication protocol stack and therefore TLS is not invoked.

6.2.1 Cryptographic Key Generation Services (FCS_CKM_EXT.1)

Asymmetric cryptographic keys are not generated by the TOE or the underlying platform. The TOE does not support any network interfaces. The evaluated configuration performs a backup and restore of the configuration database.

6.2.2 Random Bit Generation (FCS_RBG_EXT.1)

The TOE does not use any DRBG functionality. The TOE does not support any network interfaces. The TOE invokes platform-provided DPAPI and relies on BitLocker to protect data at rest.

6.2.3 Storage of Credentials (FCS_STO_EXT.1)

The TOE does not store any credentials.

6.3 User Data Protection

6.3.1 Encryption of Sensitive Application Data (FDP_DAR_EXT.1)

The TOE invokes platform-provided DPAPI and relies on platform provided BitLocker to protect data at rest. The sensitive data consists of backup files, backup copies and metadata of replicated VMs.

6.3.2 Access to Platform Resources (FDP_DEC_EXT.1)

The TOE does not access any hardware resources. The application restricts access to VBR event logs, VBR job information, and VBR infrastructure information.

6.3.3 Network Communications (FDP_NET_EXT.1)

The TOE does not have any network connectivity.

6.4 Security Management

6.4.1 Secure by Default Configuration (FMT_CFG_EXT.1)

The application is accessed by first logging onto the Windows server hosting the application. The application is installed under a platform administrative account or server account with appropriate permissions. The application does not install with default credentials.

6.4.2 Supported Configuration Mechanism (FMT_MEC_EXT.1)

Information about the PostgreSQL database (location, basic listening ports, license info and logging option) is stored within the Windows Registry.

6.4.3 Specification of Management Functions (FMT_SMF.1)

The TOE provides authorized administrators with the ability to back up and restore the configuration database. Management functions are performed by invoking the application on the system on which the TOE is installed.

6.5 Privacy

6.5.1 User Consent for Transmission of Personally Identifiable Information (FPR_ANO_EXT.1)

The TOE does not have any network interfaces and therefore does not transmit PII over the network.

6.6 Protection of the TSF

6.6.1 Anti-Exploitation Capabilities (FPT_AEX_EXT.1)

The TOE does not map memory at any explicit address. The /DYNAMICBASE link option is used to enable ASLR.

The TOE does not allocate any memory with both write and execute permissions.

The TOE can be deployed on Windows Server with the following Windows Defender Exploit Guard settings enabled:

- Control Flow Guard (CFG)
- Randomize memory allocations (Bottom-Up ASLR)
- Export address filtering (EAF)
- Import address filtering (IAF)
- Data Execution Prevention (DEP)

The TOE does not create user-modifiable files.

The TOE implements stack-based buffer overflow protection. The /GS flag was used during compilation.

6.6.2 Use of Supported Services and APIs (FPT_API_EXT.1)

The TOE invokes the Microsoft products identified in Appendix A. These products are installed by Veeam installer when VBR is installed or are part of Windows OS.

6.6.3 Software Identification and Versions (FPT_IDV_EXT.1)

SWID tags are not used. TOE versions are identified as Major.0.Minor.Build PYYYYMMDD, where each field has the following meaning:

- Major = major release with a number of significant features (architectural changes only done here)
- 0 = not used
- Minor = minor releases, usually mostly centered around new platforms version support (OS, hypervisors, app) + bug fix. Can have a few minor features/enhancements not resulting in significant product changes.
- Build = build number (goes from 1 to infinity within the given Major version)
- PYYYYMMDD = cumulative hotfix rollups, labeled with the date when patch package was built.

6.6.4 Use of Third Party Libraries (FPT_LIB_EXT.1)

The third-party libraries used in the TOE are identified in Appendix A.

6.6.5 Trusted Update (FPT_TUD_EXT.1), Integrity for Installation and Update (FPT_TUD_EXT.2)

The TOE provides the ability for authorized administrators to check for available updates. The current version of the TOE is verified by selecting the Help menu and then selecting About.

Updates must be manually downloaded and installed. Because the TOE does not support a network interface, administrators are required to check and download updates from another system and then manually load the update on the TOE hosted system.

An administrator must navigate to the Veeam KB article. https://www.veeam.com/kb4420 and compare the published latest version to that of the installed TOE. If the published version is later than the TOE version, click “Download Patch” to download the latest cumulative patch. The cumulative patch is then copied onto the TOE host system.

Veeam digitally signs the TOE installation package and TOE updates with a Veeam Software Group GmbH certificate, DigiCert is the Certificate Authority. Code is signed on the Veeam signing server during the build process.

The installation package and update/patch digital signature is verified by the Windows OS. The digital signature of the executable is also verified by the Windows platform. If something is wrong with signature, Windows displays a message with the issue and asks if the installation should proceed. If the signature fails, the administrator must terminate the update process.

The .exe file is distributed within a .iso file. The TOE is distributed and installed separately from Windows. The TOE does not download, modify, replace, or update its own binary code.

6.7 Trusted Path/Channels

6.7.1 Protection of Data in Transit (FTP_DIT_EXT.1)

The TOE does not support any network interfaces and therefore, does not provide protection of data in transit.

Per the Protection Profile definition, the TOE does not transmit any sensitive data between itself and another trusted IT product.

7. Protection Profile Claims

This ST claims exact conformance to the *Protection Profile for Application Software,* Version 1.4, 07 October 2021 (App PP) along with all applicable errata and interpretations from the certificate issuing scheme.

As explained in section 3, the Security Problem Definition of the App PP has been included by reference into this ST.

As explained in section 4, Security Objectives, the Security Objectives of the App PP has been included by reference into this ST.

All claimed SFRs are defined in the App PP. All mandatory SFRs are claimed. No optional SFRs are claimed. No objective SFRs are claimed. Selection-based SFR claims are consistent with the selections made in the mandatory SFRs that prompt their inclusion.

8. Rationale

This Security Target includes by reference the App PP Security Problem Definition, Security Objectives, and Security Assurance Requirements. The Security Target does not add, remove, or modify any of these items. Security Functional Requirements have been reproduced with the Protection Profile operations completed. All selections, assignments, and refinements made on the claimed Security Functional Requirements have been performed in a manner that is consistent with what is permitted by the App PP. The proper set of selection-based requirements have been claimed based on the selections made in the mandatory requirements. Consequently, the claims made by this Security Target are sufficient to address the TOE's security problem.

8.1 TOE Summary Specification Rationale

Table 7: Security Functions vs. Requirements Mapping

SFR	Cryptographic support	User data protection	Security management	Privacy	Protection of the TSF
FCS_CKM_EXT.1	✓				
FCS_RBG_EXT.1	✓				
FCS_STO_EXT.1	✓				
FDP_DAR_EXT.1		✓			
FDP_DEC_EXT.1		✓			
FDP_NET_EXT.1		✓			
FMT_CFG_EXT.1			✓		
FMT_MEC_EXT.1			✓		
FMT_SMF.1			✓		
FPR_ANO_EXT.1				✓	
FPT_AEX_EXT.1					✓
FPT_API_EXT.1					✓
FPT_IDV_EXT.1					✓
FPT_LIB_EXT.1					✓
FPT_TUD_EXT.1					✓
FPT_TUD_EXT.2					✓
FTP_DIT_EXT.1					✓

Appendix A TOE Usage of Third-Party Libraries

Table 8: Supported Services and APIs

Service/API	Description
PostgreSQL 15.1	Is a free and open-source relational database management system emphasizing extensibility and SQL compliance.
System Center Virtual Machine Manager (SCVMM) 2012 SP1 to 2019 Admin UI	SCVMM forms part of Microsoft's System Center line of virtual machine management and reporting tools, alongside previously established tools such as System Center Operations Manager and System Center Configuration Manager.
Microsoft .NET Framework 4.7.2	A proprietary software framework developed by Microsoft.
Windows Installer 4.5	A software component and application programming interface of Microsoft Windows used for the installation, maintenance, and removal of software.
Microsoft Windows PowerShell 5.1	PowerShell is a task automation and configuration management program from Microsoft, consisting of a command-line shell and the associated scripting language.
Microsoft SQL Server Management Objects (SMO)	SMOs are .NET objects designed to allow for easy and simple programmatic management of Microsoft SQL Server.
Microsoft SQL Server System CLR Types	A package that contains the components implementing geometry, geography and hierarchy id types in SQL Server.
Microsoft Report Viewer Redistributable 2015	Enables applications that run on the .NET Framework to display reports designed using Microsoft reporting technology.
Microsoft Universal C Runtime	A set of low-level routines used by a compiler to invoke some of the behaviors of a runtime environment by inserting calls to the runtime library into compiled executable binary.
Windows DPAPI	DPAPI (Data Protection Application Programming Interfaces) is a simple cryptographic application programming interface available as a built-in component of Windows. Its primary use is to perform symmetric encryption of asymmetric private keys.
Windows Schannel	The Secure Channel (Schannel) security package supports public-key based protocols: Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Private Communication Technology (PCT).
Window Registry	A hierarchical database that stores low-level settings for the Microsoft Windows operating system and for application that opt to use the registry.

Table 9 Third Party Libraries

Third Party Libraries	
Name	Version
@angular/animations	9.0.0
@angular/common	9.0.0
@angular/compiler	9.0.0
@angular/core	9.0.0
@angular/forms	9.0.0
@angular/platform-browser	9.0.0
@angular/platform-browser-dynamic	9.0.0
@angular/router	9.0.0
@babel/runtime	7.21.0
@clr/angular	3.0.0
@clr/city	1.1.0
@clr/core	3.0.0
@clr/icons	3.0.0
@clr/ui	3.0.0
@ngx-translate/core	11.0.1
@ngx-translate/http-loader	4.0.0
@types/element-resize-event	2.0.0
@types/history	4.7.4
@types/hoist-non-react-statics	3.3.1
@types/prop-types	15.7.5
@types/react	16.9.0
@types/react-transition-group	4.4.0
@types/react-window	1.8.2
@types/styled-components	5.1.19
@webcomponents/custom-elements	1.2.2
@webcomponents/custom-elements	1.5.1
@webcomponents/shadycss	1.11.1
@webcomponents/webcomponentsjs	2.7.0
Active Directory Authentication Library (ADAL) for .NET	5.2.9
AdaptiveCards	2.0.0
AdaptiveCards.Rendering.Html	2.0.0
AngleSharp	0.14.0
AngleSharp.Css	0.14.2
ASP.NET API Versioning	4.1.1
ASP.NET Core	6.0.7

ASP.NET MVC 5.x, Web API 2.x, Web Pages 3.x, and Razor 3.x	3.2.7
AsyncEx	5.1.2
Autofac	6.3.0
Autofac.Extensions.DependencyInjection	7.2.0
AutoMapper	10.1.1
AutoMapper	8.1.1
AutoMapper	9.0.0
AutoMapper.Extensions.EnumMapping	1.1.0
AutoMapper.Extensions.Microsoft.DependencyInjection	7.0.0
AWS SDK for .NET	3.7
Azure Active Directory IdentityModel Extensions for .NET	6.10.0
Azure Active Directory IdentityModel Extensions for .NET	6.14.1
Azure Active Directory IdentityModel Extensions for .NET	6.15.1
Azure Active Directory IdentityModel Extensions for .NET	6.16.0
Azure Active Directory IdentityModel Extensions for .NET	6.17.0
Azure Management Libraries for .NET	1.37.1
Azure Management Libraries for .NET	1.38.1
Azure.Identity	1.4.0
Azure.ResourceManager	1.3.1
Azure.Security.KeyVault.Keys	4.2.0
Azure.Storage.Files.Shares	12.8.0
Azure.Storage.Queues	12.6.0
balanced-match	1.0.2
Boost	1.76
Castle.Core	4.4.0
clarity	0.10.28
classlist.js	1.1.20150312
code-prettify	12/4/2015
core-js	2.2.0
core-js	2.6.9
cpprestsdk	2.9.0
css-vars-ponyfill	1.9.0
css-vars-ponyfill	2.4.8
csstype	2.6.2

csstype	3.1.1
custom-elements	1.1.3
debug	2.6.9
decode-uri-component	0.2.2
dedent	0.7.0
dom-helpers	5.2.1
DotLiquid	2.0.314
element-resize-event	3.0.3
EventSource	0.0.17
fast-deep-equal	2.0.1
FluentValidation	10.3.6
FluentValidation	11.1.0
FluentValidation	8.4.0
FluentValidation	8.6.1
FluentValidation	8.6.2
FluentValidation	9.2.0
FluentValidation.AspNetCore	10.3.6
FluentValidation.AspNetCore	11.1.2
FluentValidation.AspNetCore	9.2.0
FluentValidation.DependencyInjectionExtensions	10.3.6
FluentValidation.DependencyInjectionExtensions	11.1.0
FluentValidation.DependencyInjectionExtensions	9.2.0
Functional.Maybe	2.0.20
get-css-data	2.1.0
goober	2.1.1
google-gson	2.8
Google.Api.CommonProtos	2.3.0
Google.Api.Gax	3.5.0
Google.Api.Gax.Grpc	3.5.0
Google.Api.Gax.Grpc.GrpcCore	3.5.0
Google.Cloud.Billing.V1	2.3.0
Google.Cloud.Iam.V1	2.2.0
Google.Protobuf	3.15.8
Granados SSH	2.0.0
Grpc.Auth	2.38.0
Grpc.Core	2.38.1
Grpc.Core.Api	2.38.1
Hellang.Middleware.ProblemDetails	4.2.0
history	4.10.1

hoist-non-react-statics	3.3.2
Html Agility Pack	1.8.11
HtmlSanitizer	5.0.376
Hyak.Common	1.2.2
IdentityModel Extensions for .Net	5.4.0
IdentityModel Extensions for .Net	5.5.0
immer	9.0.12
Ionic.Zip	1.9.1.8
isarray	0.0.1
Jayrock	0.9.16530
JetBrains.Annotations	2022.1.0
jquery	3.6.0
jquery	3.6.0
js-tokens	4.0.0
Json.NET	12.0.3
Json.NET	13.0.1
Json.NET BSON	1.0.2
JsonSubTypes	1.6.0
libcxxrt	f2e55091e2e878386c9f7974d4922bbdc4faed84
LIBNFS	4.1
lit-element	2.5.1
lit-html	1.4.1
loose-envify	1.4.0
LZ4	1.9.2
memoize-one	5.2.1
Microsoft ASP.NET Web API 2.2 Client Libraries	5.2.7
Microsoft Authentication Library Extensions for .NET	2.18.4
Microsoft Azure Storage Client Library for C++	5.0.0
Microsoft Azure Storage SDK for .NET	9.3.2
Microsoft Prism Library for WPF	4
Microsoft SQL Server 2017 Management Objects	
Microsoft System CLR Types for Microsoft SQL Server 2017	2017.0140.1016.290
Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package ATL Security Update	
Microsoft Visual C++ 2015-2019 Redistributable (x64)	
Microsoft Visual C++ Redistributable Packages for Visual Studio 2013	
Microsoft Visual C++ Redistributable Packages for Visual Studio 2015 Update 3	
Microsoft.ApplicationInsights	2.13.1

Microsoft.AspNet.WebApi.Versioning	3.1.0
Microsoft.AspNetCore.Hosting.Abstractions	2.2.0
Microsoft.AspNetCore.Hosting.Server.Abstractions	2.2.0
Microsoft.AspNetCore.Http.Abstractions	2.2.0
Microsoft.AspNetCore.Http.Extensions	2.2.0
Microsoft.AspNetCore.Http.Features	2.2.0
Microsoft.AspNetCore.StaticFiles	2.2.0
Microsoft.Azure.ActiveDirectory.GraphClient	2.1.1
Microsoft.Azure.Amqp	2.2.0
Microsoft.Azure.Common	2.2.1
Microsoft.Azure.KeyVault	3.0.5
Microsoft.Azure.KeyVault.Core	1.0.0
Microsoft.Azure.Management.Compute	57.0.0
Microsoft.Azure.Management.ManagedServices	1.1.0
Microsoft.Azure.Management.MarketplaceOrdering	1.0.1
Microsoft.Azure.Management.ServiceBus	3.0.0
Microsoft.Azure.Services.AppAuthentication	1.0.3
Microsoft.Bcl.AsyncInterfaces	6.0.0
Microsoft.CodeAnalysis.Common	4.0.1
Microsoft.Data.Edm	5.8.4
Microsoft.Data.OData	5.8.4
Microsoft.Data.Services.Client	5.8.4
Microsoft.Diagnostics.Runtime	1.1.142101
Microsoft.Extensions.FileProviders.Abstractions	2.2.0
Microsoft.Extensions.Hosting.Abstractions	2.2.0
Microsoft.Extensions.WebEncoders	2.2.0
Microsoft.Graph	1.20.0
Microsoft.Graph	3.33.0
Microsoft.Graph.Core	1.18.0
Microsoft.Graph.Core	1.25.1
Microsoft.Graph.Core	2.0.8
Microsoft.Identity.Client.Extensions.Msal	2.18.4
Microsoft.MarkedNet	1.0.13
Microsoft.Net.Http.Headers	2.2.0
Microsoft.OpenApi	1.1.4
Microsoft.OpenApi	1.2.3
Microsoft.Owin	4.1.0
Microsoft.Rest.ClientRuntime	2.3.23
Microsoft.Rest.ClientRuntime.Azure	3.3.18

Microsoft.Rest.ClientRuntime.Azure.Authentication	2.4.1
Microsoft.SqlServer.SqlManagementObjects	160.2004021.0
Microsoft.Toolkit.Uwp.Notifications	6.1.0
Microsoft.Xaml.Behaviors.Wpf	1.1.39
MimeKitLite	3.1.1
moment	2.29.4
moment-duration-format	2.3.2
ms	2.0.0
mutationobserver-shim	0.3.2
Namotion.Reflection	1.0.8
Newtonsoft.Json	12.0.3
ng2-charts	1.6.0
Nito.Cancellation	1.1.2
Nito.Collections.Deque	1.1.1
Nito.Disposables	2.2.1
NJsonSchema	10.1.4
NJsonSchema	9.14.1
NJsonSchema.CodeGeneration	10.1.4
NJsonSchema.CodeGeneration.CSharp	10.1.4
NLog	4.7.9
Npgsql	6.0.5
Npgsql	6.0.7
NSwag	12.3.1
NSwag	13.2.2
object-assign	4.1.1
OneOf	3.0.201
OpenSSL	1.0.2ze
Owin	1.0.0
path-to-regexp	1.8.0
plural-forms	0.5.3
PnP.Core	1.3.0
PnP.Framework	1.6.0
Polly	7.2.2
Polly.Extensions.Http	3.0.0
Portable.BouncyCastle	1.9.0
Portable.Xaml	0.26.0
prettify	r298
Prism	6.2.0
Prism	7.1.0

Prism.Core	8.1.97
prop-types	15.8.1
Putty	0.74
Putty	0.76
query-string	5.1.1
QuikGraph	2.3.0
react	16.9.0
react-dom	16.9.0
react-is	16.13.1
react-transition-group	4.4.1
react-window	1.8.5
Rebex.Elliptic.Castle	1.2.1
Rebex.Elliptic.Curve25519	1.2.1
Rebex.Elliptic.Ed25519	1.2.1
regenerator-runtime	0.13.11
Renci.SshNet.Async	1.4.0
resolve-pathname	3.0.0
ResXResourceReader.NetStandard	1.0.0
routr	2.1.2
rxjs	5.5.0
rxjs	6.5.2
rxjs	6.5.4
scheduler	0.15.0
Scrutor	3.0.2
SharePoint and Project Client Object Model libraries	16.1.21714.12000
SharePoint PnP Core library for SharePoint Online	3.28.2012
SharePointPnP.IdentityModel.Extensions	1.2.4
sharpBits.Net	N/A
SharpYaml	1.6.5
signalr	2.4.2
SimpleJSON	N/A
SSH.NET	2016.1.0
SSH.NET	2020.0.2
SshNet.Security.Cryptography	1.3.0
StdString.h	no version, the latest update in the file: 2005-APR-01
strict-uri-encode	1.1.0
swagger-ui	4.13.1
swagger-ui	4.13.2

Swashbuckle	5.5.3
Swashbuckle.AspNetCore	5.0.0
Swashbuckle.AspNetCore	6.2.3
Swashbuckle.AspNetCore	6.3.2
System.CodeDom	5.0.0
System.Collections.Immutable	5.0.0
System.Linq.Async	5.0.0
System.Net.Http.WinHttpHandler	6.0.0
System.Reactive	4.4.1
System.Reflection.Metadata	5.0.0
System.Runtime.CompilerServices.Unsafe	5.0.0
System.Runtime.CompilerServices.Unsafe	6.0.0
System.ServiceProcess.ServiceController	4.7.0
System.Spatial	5.8.4
System.Text.Encodings.Web	6.0.0
System.Text.Json	6.0.2
System.ValueTuple	4.5.0
TimeZoneConverter	3.5.0
tiny-invariant	1.3.1
tiny-warning	1.0.3
ts-helpers	1.1.2
tslib	1.10.0
tslib	1.14.1
ttag	1.7.24
Unity Container	5.11.1
utf8.h, utf8/checked.h, utf8/unchecked.h, utf8/core.h	
value-equal	1.0.1
web-animations-js	2.3.2
WebSocket++	0.5.1
wiasane	0.0.0.5
Windows 10 SDK	10.0.18362.1
Windows 10 SDK	version 1803 (10.0.17134.12)
WindowsAzure.Storage	6.0.0
zlib	1.2.13
zone.js	0.10.3
zone.js	0.8.20
zstd	1.5.2