Veeam ONE 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

Table of Contents

List of Figures and Tables

1 Security Target Introduction

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

- 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 ONE v12 Security Target

ST Version: 1.6

ST Date: 9 July 2023

Target of Evaluation (TOE) Identification Veeam ONE v12

TOE Version: 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 specification:

- *Protection Profile for Application Software,* Version 1.4, 7 October 2021 (App PP) with the following selection-based SFR:
  - 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 considered 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 FIA_X509_EXT.1 is not claimed.
0717	Format changes for PP_APP_V1.4.	Applicable because the ST claims conformance to the App PP.
0719	ECD for PP APP 1.3 and 1.4.	Applicable because the ST claims conformance to the App PP.
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 ("/") and text at the end of the component. For example, FCS_COP.1/* indicates that the ST includes iterations of the FCS_COP.1 requirement.
  - 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., [<u>selection item</u>]).
  - 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.

1.4 Acronyms

Table 2: Acronyms

Term	Definition
API	Application Programming Interface
ASLR	Address Space Layout Randomization
CC	Common Criteria for Information Technology Security Evaluation
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman (Ephemeral)
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GB	Gigabyte
IIS	Internet Information Services
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PP	Protection Profile
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

Term	Definition
VBR	Veeam Backup and Replication

2 TOE Description

2.1 Product Overview

The Veeam Availability Suite™ is a software 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 ONE 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 claimed requirements claimed in this ST.

2.2 TOE Overview

Veeam® ONE™, a part of the Veeam Availability Suite™ provides a monitoring and analytics solution for backup, virtual and physical environments, providing support for Veeam Backup & Replication™ and Veeam Agents, as well as VMware, Hyper-V and Nutanix AHV.

Veeam ONE features include:

- Built-in Intelligence: Identify and resolve common infrastructure and software misconfigurations before operational impact.
- Governance & Compliance: Organizations know their data protection posture instantly through consistent monitoring and reporting on backup SLA compliance.
- Intelligent Automation: Machine Learning-based diagnostics as well as remediation actions to resolve issues faster.
- Forecasting and planning: Visibility into the costs of compute, storage, and backup repository resources to forecast utilization rates and resource requirements.

2.3 TOE Architecture

Veeam ONE relies on a client-server architecture to work effectively in environments of any size and complexity. The Veeam ONE architecture includes the following structural components:

- **Veeam ONE Server**: Veeam ONE Server is responsible for collecting data from virtual and Veeam Backup & Replication servers and storing this data into the database. As part of Veeam ONE Server, the following components are installed:
  - Veeam ONE Monitoring Service,
  - Veeam ONE Reporting Service,
  - Veeam ONE Error Reporting Service, and
  - Veeam ONE Web API.
- **Veeam ONE Web Services**: Veeam ONE Web Services enable access to Veeam ONE web server and handle rendering of reports.

- **Veeam ONE Client**: Veeam ONE Client is a client part for Veeam ONE Server. Veeam ONE Client communicates with the Veeam ONE Server to obtain real-time virtual infrastructure performance data and data protection statistics.
- **Veeam ONE Agent**: Veeam ONE agent is a component that enables communication with Veeam Backup & Replication servers, performs collection of event logs and infrastructure information, and sends remediation commands.

  Veeam ONE Agent can work in the following modes:

  - **Server**: In this mode, Veeam ONE agent is responsible for analyzing VBR event log data, infrastructure information and signature updates.

    Veeam ONE Agent Server is included into Veeam ONE installation package and deployed on the machine running Veeam ONE Server during product installation.

  - **Client**: In this mode, Veeam ONE agent is responsible for collecting logs and executing remediation actions on Veeam Backup & Replication servers.

  Only Veeam ONE Agent configured in Server mode is in scope for this evaluation.

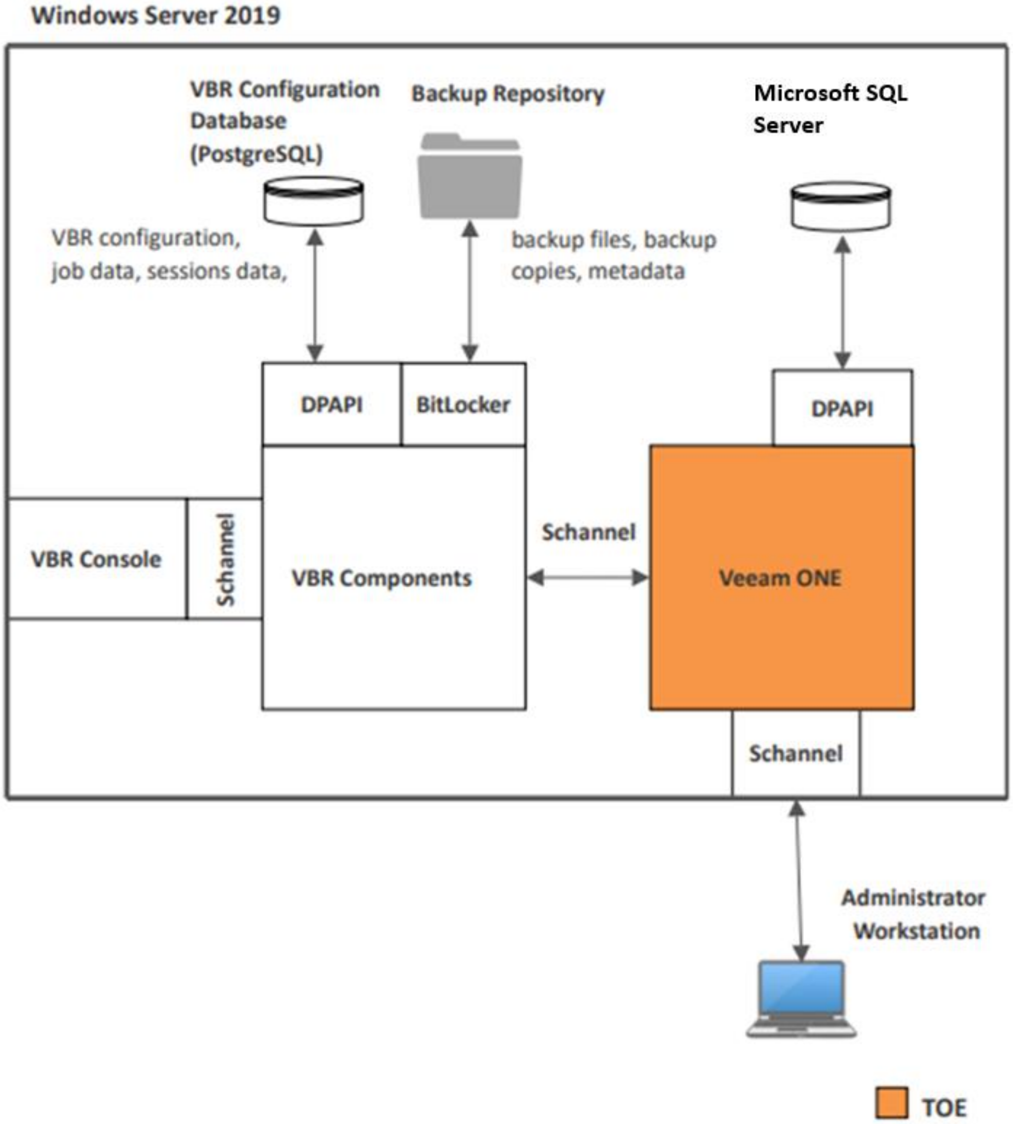
- **Veeam ONE Web Client** provides a set of dashboards and reports that allow an administrator to verify configuration issues, optimize resource allocation and utilization, track implemented changes, plan capacity growth and track whether workloads are properly protected in the virtualized datacenter.

Veeam ONE's supporting environment includes the following systems.

- **Veeam Backup & Replication host:** runs the VBR application.
- **Microsoft SQL Server**: Veeam ONE database is hosted on a Microsoft SQL Server that can run remotely or can be co-installed with other Veeam ONE components. The repository stores data used by product components.
- **Windows Workstation:** connects to Veeam ONE to view event logs and infrastructure information.

2.3.1 Physical Boundary

Figure 1: Veeam ONE TOE Physical Boundary


Windows Server 2019
VBR Configuration Database (PostgreSQL)
Backup Repository
Microsoft SQL Server
VBR configuration, job data, sessions data,
backup files, backup copies, metadata
DPAPI
BitLocker
DPAPI
VBR Console
Schannel
VBR Components
Schannel
Veeam ONE
Schannel
Administrator Workstation
TOE

The Veeam ONE TOE is a set of Veeam software components that are installed on a Windows-based physical machine. The figure above depicts the TOE components in relationship to the platform provided functionality.

The Veeam ONE Components included in the TOE and described in section 2.3 TOE Architecture above are:

- **Veeam ONE Server**
- **Veeam ONE Web Services**
- **Veeam ONE Client**

- **Veeam ONE Agent**

The Microsoft SQL Server hosting the **Veeam ONE Database** described in section 2.3 is not included in the TOE boundary.

Platform provided Windows Data Protection Application Programming Interface (DPAPI) is used to store Veeam ONE configuration information in the Veeam ONE Database (SQL).

Platform provided HTTPS (Schannel) is used to enable a remote client to connect to the TOE.

The TOE connects to VBR hosts using platform provided Schannel. This is a localhost connection in the evaluated configuration and therefore, this connection does not access the protocol stack.

2.3.1.1 Evaluated Configuration

For this evaluation, the TOE and Microsoft SQL Server (providing the database for Veeam ONE) are installed on a single Windows Server.

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

Table 3: Windows Server Minimum Requirements for Veeam ONE

Item	Minimum Requirements
CPU	8 vCPUs (minimum) – 16 vCPUs (recommended) for Veeam ONE Server, Microsoft SQL Server (Veeam ONE Database).
Memory	8 GB (minimum) – 16 GB (recommended) for Veeam ONE Server, Microsoft SQL Server (Veeam ONE Database)
Hard Disk Space	50 GB for product operation and Microsoft SQL Server (Veeam ONE Database)
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2019
Software	The following components are included in the Veeam ONE setup package and can be installed automatically: • Microsoft .NET Framework 4.7.2 • Microsoft .NET Runtime 6.0.14 • Microsoft Visual C++ 2015-2019 Redistributable (x64) • Microsoft System CLR Types for SQL Server 2014 • Microsoft SQL Native Client 2012 • Microsoft SQL Server 2014 Management Objects • Microsoft SQL Server 2012 Management Objects • Microsoft OLE DB Driver for SQL Server • Microsoft XML 6.0 Parser and SDK • Microsoft ASP.NET Core Shared Framework 6.0.14 • Microsoft Universal C Runtime • Microsoft SQL Server 2016 (Microsoft SQL Server 2016 Express edition is included in Veeam ONE 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.

CAVP certificate A2014 identifies Microsoft Windows Server 2019 (64-bit) on Intel Xeon Silver 4114 with AES-NI and without SHA extensions. The Intel Xeon Silver 4114 also implements the Skylake microarchitecture. Therefore, for the purpose of this evaluation the processors may be considered equivalent.

The following requirements must be satisfied by other equipment in the OE.

Table 4: OE Components Minimum Requirements

Required Item	Veeam ONE Infrastructure Component	Description
A Workstation	A computer with a web browser.	Used for a remote connection that the administrator uses to connect to the Veeam ONE UI.

Required Item	Veeam ONE Infrastructure Component	Description
Microsoft SQL Server		Veeam ONE database is hosted on a Microsoft SQL Server that can run remotely or can be co-installed with other Veeam ONE components. The repository stores data used by product components. For this evaluation both Microsoft SQL Server and Veeam are installed on the same host.
Veeam Backup and Replication v12	One instance of VBR.	One instance of VBR. Veeam ONE connects to VBR to retrieve event logs about backup and recovery tasks performed by VBR and infrastructure information of the hosts VBR connects to. For this evaluation both VBR and Veeam are installed on the same host.

2.3.1.2 Functionality Excluded from the Evaluated Configuration

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

- Veeam ONE includes the ability to monitor Veeam Backup & Replication (VBR) and VMware vSphere, VMware vCloud Director and Microsoft Hyper-V. Only monitoring of VBR is included in the evaluated configuration.
- Veeam ONE Agent in Client mode is excluded from the evaluated configuration. Per Section 2.3, the TOE does not include a “Veeam ONE Agent Client”, just “Veeam ONE Agent”.

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 in transit and at rest.

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 SQL 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 and remote administration via the platform-provided web server (IIS). Users must login to Windows and have permissions to access the UI in order to access the TOE.

Administrators may configure which VBR instances have their Event Logs analyzed by the TOE, and access reports resulting from that analysis.

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, 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. Availability of updates is announced via email sent to customers as well as via the Veeam website.

2.3.2.6 Trusted Path/Channels

The TOE protects data in transit with remote administrators by invoking the platform-provided IIS.

2.4 TOE Documentation

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

- Monitoring Guide: Veeam ONE Version 12, Monitoring Guide, July, 2023
- Reporting Guide: Veeam ONE Version 12, Reporting Guide, July, 2023
- Quick Start Guide: Veeam ONE Version 12 Quick Start Guide May, 2023
- Deployment Guide: Veeam ONE Version 12, Deployment Guide, July, 2023
- Common Criteria Hardening Guide for v12
- Veeam ONE v12 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, Revision Date: July 10, 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.

This threat model is applicable to the TOE because VM data is transferred across the network and stored. It is also 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 7, 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 Requirements

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 Update
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_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1[1] The application shall [

generate no asymmetric cryptographic keys].

5.2.1.2 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The application shall [

- use no DRBG functionality,

] for its cryptographic operations.

[1] This SFR is updated by TD0717.

5.2.1.3 FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [

- invoke the functionality provided by the platform to securely store [*VBR server credentials, TLS server certificate*]

] 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 [

- protect sensitive data in accordance with FCS_STO_EXT.1

] 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 [

- network connectivity

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- [*VBR event logs and infrastructure information*]

].

5.2.2.3 FDP_NET_EXT.1 Network Communications (FDP_NET_EXT.1)

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- respond to [*incoming administrator sessions (platform-provided HTTPS)*],

] .

Application Note: *The TOE calls platform-provided Schannel to communicate with VBR. The connection is to localhost and therefore does not reach the protocol stack.*

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[2] 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 [

- [*configure the VBR systems whose event logs are analyzed, review reports of the analyzed event logs and infrastructure information*]

].

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 FPT_AEX_EXT.1 Anti-Exploitation Capabilities

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.

[2] This SFR addresses TD0624.

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 Trusted 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[3] The application shall be distributed using [the format of the platform-supported package manager].

FPT_TUD_EXT.2.2[4] 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.

[3] This SFR is modified by TD0628.

[4] This SFR addressed TD0664.

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[5] The application shall [

- invoke platform-provided functionality to encrypt all transmitted data with [HTTPS] for [*remote administration*]

] between itself and another trusted IT product.

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

6 TOE Summary Specification

This chapter describes the security functions.

6.1 Timely Security Updates ALC_TSU_EXT.1

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.

[5] This SFR addressed TD0743.

6.2 Cryptographic Support

6.2.1 Cryptographic Key Generation Services (FCS_CKM_EXT.1)

The TOE does not generate asymmetric cryptographic keys. The TOE invokes the third-party Windows Schannel library to call platform-provided functionality to provide asymmetric key generation. Schannel is used to establish a session with remote administrators connecting to the platform-provided Web Server using HTTPS.

The Microsoft Windows Server 2019 is limited to the following cipher suites as configured using the CC Hardening Guide for 12a.

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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.

CAVP certificate A2014 identifies Microsoft Windows Server 2019 (64-bit) on Intel Xeon Silver 4114 with AES-NI and without SHA extensions. The Intel Xeon Silver 4114 also implements the Skylake microarchitecture. Therefore, for the purpose of this evaluation the processors may be considered equivalent.

CAVP Certificate A2014

Function	Standard	Certificate
ECC Key Generation (P-384)	FIPS PUB 186-4	A2014
DSA Key Generation	FIPS PUB 186-4	A2014
Key Agreement Scheme FFC	SP800-56Ar3	A2014
RSA Signature Generation	FIPS186-4	A2014
RSA Signature Verification	FIPS186-4	A2014
ECDSA Signature Generation	FIPS186-4	A2014
ECDSA Signature Verification	FIPS186-4	A2014
ECC Based Key Establishment	NIST SP 800-56A	A2014
AES-GCM (256 bits)	NIST SP 800-38D	A2014
SHA-384	FIPS PUB 180-4	A2014
HMAC-SHA2-384	FIPS PUB 198-1, FIPS PUB 180-4	A2014

6.2.2 Random Bit Generation (FCS_RBG_EXT.1)

Windows DRBG functionality is not directly invoked. It is indirectly invoked by initiating an Schannel (TLS) connection and securely storing credentials (DPAPI).

6.2.3 Storage of Credentials (FCS_STO_EXT.1)

The TOE uses the following credentials:

- TLS certificate used with the platform-provided Web server (HTTPS) – stored in Windows Certificate Store.
- VBR server credentials.

6.3 User Data Protection

6.3.1 Encryption of Sensitive Application Data (FDP_DAR_EXT.1)

The only sensitive data that the TOE processes are VBR credentials. Veeam ONE uses MS SQL database to store VBR credentials. Credentials are encrypted using DPAPI mechanism.

6.3.2 Access to Platform Resources (FDP_DEC_EXT.1)

The TOE accesses network connectivity and VBR event logs and infrastructure information.

6.3.3 Network Communications (FDP_NET_EXT.1)

The TOE uses network connectivity for:

- Receiving Web Server (HTTPS) connections on port 1239 for remote administration.

6.4 Security Management

6.4.1 Secure by Default Configuration (FMT_CFG_EXT.1)

There are no administrator credentials for accessing the Veeam ONE Client. The application is accessed by first logging onto the Windows server hosting the application. The administrator navigates to the Microsoft Windows Programs menu and selects Veeam ONE Client. To connect using the account under which the administrator is logged on to the machine, select the Use Windows session credentials check box, and click Connect.

The application is installed under an admin account or server account with appropriate permissions. A user must be a member of the Veeam ONE Administrators, Veeam ONE Read-Only Users or Veeam ONE Power Users group on the system where Veeam ONE is installed.

The Veeam ONE Web Client can be accessed locally, on the machine where the Veeam ONE Web Services component is installed. Navigate to the Microsoft Windows Programs menu choose Veeam ONE Web Client.

The Veeam ONE Web Client console can be accessed using a web browser on a remote machine. To access the Veeam ONE Web Client console remotely, a user must be a member of the Veeam ONE

Administrators, Veeam ONE Read-Only Users or Veeam ONE Power Users group on the machines where Veeam ONE Web Services and Veeam ONE Server components are installed.

6.4.2 Supported Configuration Mechanism (FMT_MEC_EXT.1)

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

VBR event logs and infrastructure information are saved under the Windows Program Data folder.

6.4.3 Specification of Management Functions (FMT_SMF.1)

The TOE provides authorized administrators with the ability to configure retrieval and analysis of VBR event logs and infrastructure information from VBR systems, and review reports that the TOE generates concerning the analyzed event logs and infrastructure. Users access the TOE using a remote web UI with platform-provided HTTPS (Schannel).

6.5 Privacy

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

The network does not transmit PII over the network.

6.6 Protection of the TSF

6.6.1 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 Veeam ONE is installed or are part of Windows OS.

6.6.2 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 application runs as Managed Code in the .NET Framework and therefore does not require stack protections.

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)

The TOE provides the ability for authorized administrators to check for available updates. The TOE does not download, modify, replace, or update its own binary code. Updates must be manually downloaded and installed.

The product version number is displayed in the application by selecting the Help menu and then selecting About.

Veeam One is signed by Veeam Software Group GmbH certificate, DigiCert is Certificate Authority in this case. Code is signed on the Veeam signing server during the build process.

The TOE is distributed and installed separately from Windows.

6.6.6 Integrity for Installation and Update (FPT_TUD_EXT.2)

Veeam One is signed by Veeam Software Group GmbH certificate, DigiCert is Certificate Authority in this case. Code is signed on the Veeam signing server during the build process.

The .exe file is distributed within a .iso file.

6.7 Trusted Path/Channels

6.7.1 Protection of Data in Transit (FTP_DIT_EXT.1)

The TOE invokes Windows functionality for:

- Receiving Web Server (HTTPS) connections on port 1239 for remote administration. The TOE invokes platform provided S-channel for the secure connection.

7 Protection Profile Claims

This ST claims exact conformance to the *Protection Profile for Application Software,* Version 1.4, 7 October 2021 along with all applicable errata and interpretations from the certificate issuing scheme.

As explained in section 3, Security Problem Definition, 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 or 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**	**Identification and authentication**	**Security management**	**Privacy**	**Protection of the TSF**	**Trusted path/channels**
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
Microsoft SQL Server 2016 (Microsoft SQL Server 2016 SP2 Express Edition is included in the setup)	A relational database management system developed by Microsoft.
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 Library	Version

.NET Core Libraries (CoreFX)	2.1.0
@babel/code-frame	7.18.6
@babel/generator	7.19.6
@babel/helper-annotate-as-pure	7.18.6
@babel/helper-environment-visitor	7.18.9
@babel/helper-function-name	7.19.0
@babel/helper-hoist-variables	7.18.6
@babel/helper-module-imports	7.18.6
@babel/helper-split-export-declaration	7.18.6
@babel/helper-string-parser	7.19.4
@babel/helper-validator-identifier	7.19.1
@babel/highlight	7.18.6
@babel/parser	7.19.6
@babel/runtime	7.19.4
@babel/runtime	7.21.0
@babel/template	7.18.10
@babel/traverse	7.19.6
@babel/types	7.19.4
@emotion/is-prop-valid	0.8.8
@emotion/memoize	0.7.4
@emotion/stylis	0.8.5
@emotion/unitless	0.7.5
@jridgewell/gen-mapping	0.3.2
@jridgewell/resolve-uri	3.1.0
@jridgewell/set-array	1.1.2
@jridgewell/sourcemap-codec	1.4.14

@jridgewell/trace-mapping	0.3.17
@microsoft/signalr	6.0.10
@microsoft/signalr	6.0.15
@react-dnd/asap	4.0.1
@react-dnd/invariant	2.0.0
@react-dnd/shallowequal	2.0.0
@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	18.0.23
@types/react-transition-group	4.4.0
@types/react-transition-group	4.4.5
@types/react-window	1.8.2
@types/react-window	1.8.5
@types/scheduler	0.16.2
@types/styled-components	5.1.19
abort-controller	3.0.0
AjaxMin	5.14
ansi-styles	3.2.1
Antlr3.Runtime	3.5.0.2
Appccelerate.StateMachine	4.4.0
ASP.NET Core	6.0.14
Autofac	6.3.0
Autofac.Extensions.DependencyInjection	7.2.0
AutoMapper	10.1.1

Azure Active Directory IdentityModel Extensions for .NET	6.25.0
babel-plugin-styled-components	2.0.7
babel-plugin-syntax-jsx	6.18.0
Boost	1.77
camelize	1.0.1
CefSharp	89.0.170
chalk	2.4.2
ChartDirector	5.1.1
clsx	1.2.1
color-convert	1.9.3
color-name	1.1.3
css-color-keywords	1.0.0
css-to-react-native	3.0.0
csstype	3.1.1
date-fns	2.29.3
debug	2.6.9
debug	4.3.4
decode-uri-component	0.2.0
decode-uri-component	0.2.2
dnd-core	14.0.1
dom-helpers	5.2.1
element-resize-event	3.0.3
element-resize-event	3.0.6
EntityFramework	6.4.4
escape-string-regexp	1.0.5
event-target-shim	5.0.1

eventsource	1.1.2
fast-deep-equal	3.1.3
FastColoredTextBox.Net5	2.16.26
fetch-cookie	0.11.0
globals	11.12.0
goober	2.1.1
Google.Protobuf	3.19.1
Google.Protobuf	3.21.9
Grpc.AspNetCore.Server	2.41.0
Grpc.Core	2.41.1
Grpc.Core.Api	2.41.1
Grpc.Net.Common	2.41.0
has-flag	3.0.0
history	4.10.1
history	4.9.0
hoist-non-react-statics	3.3.2
HTMLayout	3.3.3.13
IdentityModel Extensions for .Net	5.5.0
immer	9.0.12
isarray	0.0.1
js-tokens	4.0.0
jsesc	2.5.2
Json.NET	13.0.1
Json.NET BSON	1.0.2
Lextm.SharpSnmpLib	12.4.0
lodash	4.17.21

lodash.isequal	4.5.0
loose-envify	1.4.0
MailKit	2.15.0
memoize-one	5.2.1
Microsoft ASP.NET Web Optimization Framework	1.1.3
MICROSOFT ASP.NET WEB PAGES	1.0.20105.407
Microsoft System CLR Types for Microsoft SQL Server 2017	2017.0140.1016.290
Microsoft.AspNet.FriendlyUrls	1.0.2
Microsoft.AspNet.Web.Optimization.WebForms	1.1.1
Microsoft.Bcl.AsyncInterfaces	1.0.0
Microsoft.Bcl.AsyncInterfaces	6.0.0
Microsoft.Data.SqlClient	1.1.2
Microsoft.EntityFrameworkCore	2.2.6
Microsoft.EntityFrameworkCore.Abstractions	2.2.6
Microsoft.EntityFrameworkCore.Design	2.2.6
Microsoft.EntityFrameworkCore.SqlServer	2.2.6
Microsoft.Extensions.Caching.Abstractions	2.2.0
Microsoft.Extensions.Caching.Memory	2.2.0
Microsoft.Extensions.Configuration	2.2.0
Microsoft.Extensions.Configuration.Abstractions	2.2.0
Microsoft.Extensions.Configuration.Binder	2.2.0
Microsoft.Extensions.DependencyInjection	2.2.0
Microsoft.Extensions.DependencyInjection.Abstractions	2.2.0
Microsoft.Extensions.Logging	2.2.0
Microsoft.Extensions.Logging.Abstractions	2.2.0
Microsoft.Extensions.Options	2.2.0

Microsoft.Extensions.Primitives	2.0.0
Microsoft.Identity.Client	3.0.8
Microsoft.OpenApi	1.2.3
Microsoft.ReportingServices.ReportViewerControl.WebForms	150.1400.0
MimeKit	2.15.0
ms	2.0.0
ms	2.1.2
NLog	4.7.14
node-fetch	2.6.9
NSspi	0.3.1
object-assign	4.1.1
Open Sans	
path-to-regexp	1.8.0
picomatch	2.3.1
Portable.BouncyCastle	1.8.10
postcss-value-parser	4.2.0
prop-types	15.8.1
psl	1.9.0
punycode	2.1.1
Putty	0.77
query-string	5.1.1
querystringify	2.2.0
Re-linq	2.2.0
react	16.14.0
react	18.2.0
react-dnd	14.0.5

react-dnd-html5-backend	14.1.0
react-dom	16.14.0
react-dom	18.2.0
react-draggable	4.4.5
react-grid-layout	1.3.4
react-is	16.13.1
react-resizable	3.0.4
react-transition-group	4.4.1
react-transition-group	4.4.5
react-window	1.8.5
react-window	1.8.8
redux	4.2.0
regenerator-runtime	0.13.10
regenerator-runtime	0.13.11
requires-port	1.0.0
resolve-pathname	2.2.0
resolve-pathname	3.0.0
routr	2.1.2
rxjs	7.1.0
scheduler	0.19.1
scheduler	0.23.0
Serilog	2.11.0
SerilogWeb.Classic	5.1.66
shallowequal	1.1.0
SnmpSharpNet	0.9.5
sprintf	1.0.3

stateless	5.11.0
strict-uri-encode	1.1.0
styled-components	5.3.3
supports-color	5.5.0
Swashbuckle.AspNetCore.Annotations	6.3.0
Swashbuckle.AspNetCore.Swagger	6.3.0
Swashbuckle.AspNetCore.SwaggerGen	6.3.0
Swashbuckle.AspNetCore.SwaggerUI	6.3.0
System.Collections.Immutable	1.7.1
System.Runtime.CompilerServices.Unsafe	6.0.0
System.Text.Encodings.Web	6.0.0
System.Text.Json	4.7.2
System.Text.Json	6.0.2
System.ValueTuple	4.5.0
tiny-invariant	1.3.1
tiny-warning	1.0.3
to-fast-properties	2.0.0
tough-cookie	4.1.2
tr46	0.0.3
tslib	1.13.0
tslib	2.1.0
tslib	2.1.0
tslib	2.4.0
universalify	0.2.0
url-parse	1.5.10
value-equal	0.4.0

value-equal	1.0.1
WebGrease	1.6.0
webidl-conversions	3.0.1
whatwg-url	5.0.0
ws	7.5.9