

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**



Validation Report

for

One Identity Safeguard for Privileged Sessions 6.9

Report Number: CCEVS-VR-VID11214-2022

Dated: 04 March 2022

Version: 1.0

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

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

Acknowledgements

Validation Team

Patrick Mallett, PhD

Jerome Myers, PhD

Marybeth Panock

The Aerospace Corporation

Common Criteria Testing Laboratory

*Leidos Inc.
Columbia, MD*

Contents

1	Executive Summary.....	1
2	Identification.....	2
3	TOE Architecture.....	4
4	Security Policy.....	5
4.1	Security Audit.....	5
4.2	Cryptographic Support.....	5
4.3	Identification and Authentication.....	5
4.4	Security Management.....	5
4.5	Protection of the TSF.....	5
4.6	TOE Access.....	5
4.7	Trusted Path/Channels.....	5
5	Assumptions and Clarification of Scope.....	6
5.1	Assumptions.....	6
5.2	Clarification of Scope.....	7
6	Documentation.....	8
7	IT Product Testing.....	9
7.1	Test Configuration.....	9
8	TOE Evaluated Configuration.....	12
8.1	Evaluated Configuration.....	12
8.2	Excluded Functionality.....	12
9	Results of the Evaluation.....	14
9.1	Evaluation of the Security Target (ST) (ASE).....	14
9.2	Evaluation of the Development (ADV).....	14
9.3	Evaluation of the Guidance Documents (AGD).....	14
9.4	Evaluation of the Life Cycle Support Activities (ALC).....	14
9.5	Evaluation of the Test Documentation and the Test Activity (ATE).....	15
9.6	Vulnerability Assessment Activity (AVA).....	15
9.7	Summary of Evaluation Results.....	15
10	Validator Comments/Recommendations.....	16
11	Security Target.....	17
12	Abbreviations and Acronyms.....	18
13	Bibliography.....	19

List of Tables

Table 1: Evaluation Identifiers	2
---------------------------------	---

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of One Identity Safeguard for Privileged Sessions 6.9 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

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

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in March 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant

and demonstrates exact conformance to:

- *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020*

as clarified by all applicable Technical Decisions.

The TOE is One Identity Safeguard for Privileged Sessions 6.9.

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

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

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST.

2 Identification

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

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	One Identity Safeguard for Privileged Sessions 6.9
Security Target	One Identity Safeguard for Privileged Sessions 6.9 Security Target, Version 1.0, 20 January 2022
Sponsor & Developer	One Identity 4 Polaris Way Aliso Viejo, CA 92656
Completion Date	March 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Evaluation Personnel	Justin Fisher Pascal Patin Furukh Siddique
Validation Personnel	Patrick Mallett Jerome Myers Marybeth Panock

3 TOE Architecture

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

The TOE is a standalone network device consisting of a hardware appliance (3000/3500) pre-installed with the One Identity Safeguard for Privileged Sessions (SPS) 6.9 software/firmware. The SPS software/firmware is based on Ubuntu Linux LTS 18.04, hardened according to the official Ubuntu guides. The appliance is installed in-line between clients and servers to facilitate communications and enforce access control, authorization, and accounting methods on application-layer protocols. The TOE supports local and remote administration. The TOE provides Web UI and REST API management interfaces that an administrator can access via Ethernet ports as well as a local console that can be accessed via serial port. Remote administration is protected using HTTPS.

The TOE provides a local password-based identification and authentication method for its local and remote administrative interfaces. Authentication for remote interfaces can also be configured to use LDAP/AD password-based authentication.

The TOE is evaluated as a network device offering CAVP certified cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections with external IT entities (assets and audit server), protected using SSH, TLS, or HTTPS.

4 Security Policy

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

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

4.1 Security Audit

The TOE generates security relevant audit records, stores them locally, and can be configured to forward them to a syslog server over TLS. The locally stored audit records are protected from unauthorized access.

4.2 Cryptographic Support

The TOE uses OpenSSL with NIST-validated algorithm implementations in support of its cryptographic functions. The TOE uses these algorithms to implement TLS, HTTPS, and SSH in accordance with defined standards.

4.3 Identification and Authentication

The TOE provides identification and authentication and password management functions for its administrative interface. It also supports X.509 certificate services in support of authentication for cryptographic channels, including certificate revocation checking using CRL.

4.4 Security Management

The TOE provides security management functions and defines roles that can be associated with users in order to manage the TOE locally or remotely. The management functions are provided through a Web UI, REST API, and local Console.

4.5 Protection of the TSF

The TOE implements features designed to protect itself to ensure the reliability and integrity of its security features to include protecting sensitive data and providing its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE includes functions to perform self-tests so that it can detect when it is failing and transition to a secure, maintenance state. It also includes a mechanism to verify TOE updates to prevent malicious or other unexpected changes in the TOE.

4.6 TOE Access

The TOE displays a Security Administrator-specified advisory notice and consent warning message prior to establishing an administrative user session. The TOE terminates local and remote administrator interactive sessions after a Security Administrator-specified time period of inactivity. The TOE allows administrator-initiated termination of the administrator's own interactive session.

4.7 Trusted Path/Channels

The TOE provides trusted paths and channels for remote administrators and trusted IT entities. The TOE can be configured to send audit records to external syslog server(s) using TLS in real-time.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For virtual Network Devices (vNDs), this assumption applies to the physical platform on which the virtual machine (VM) runs.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

In the case of vNDs, the virtualization system (VS) is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.

- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

- The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Clarification of Scope

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

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019* and performed by the evaluation team).
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in One Identity Safeguard for Privileged Sessions 6.9 Security Target, Version 1.0, 20 January 2022. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious”, vulnerabilities to objectives not claimed in the ST, or vulnerabilities that would explicitly require a violation of the assumptions claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

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

- One Identity Safeguard for Privileged Sessions 6.9.3 Common Criteria Evaluated Configuration Guidance (CCECG), Version 1.1, January 26, 2022
- One Identity Safeguard for Privileged Sessions 6.9.3 Administration Guide, April 30, 2021
- One Identity Safeguard for Privileged Sessions 6.9.3 Installation Guide, April 30, 2021
- One Identity Safeguard for Privileged Sessions 6.9.3 REST API Reference Guide, April 30, 2021
- One Identity Safeguard for Privileged Sessions 6.9.3 Packaging Checklist, April 30, 2021
- One Identity Safeguard for Privileged Sessions 6.9.3 Upgrade Guide, April 30, 2021
- Super SC113 Chassis Series User's Manual, Version 1.0d.
- Supermicro SuperServer 1029U-T Series User's Manual, Revision 1.0i
- Super X9 SMT IPMI User Guide, Revision 1.0
- One Identity Safeguard for Privileged Sessions 6.9.4 Release Notes, 27 January 2022

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

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

7 IT Product Testing

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

- *One Identity Safeguard for Privileged Sessions 6.9 Common Criteria Test Report and Procedures, Version 1.1, 28 February 2022*

A non-proprietary description of the tests performed, and their results is provided in Section 3.5 of the following document:

- *Assurance Activities Report for One Identity Safeguard for Privileged Sessions 6.9, Version 1.0, 28 February 2022*

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020*.

The evaluation team devised a Test Plan based on the Test Activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

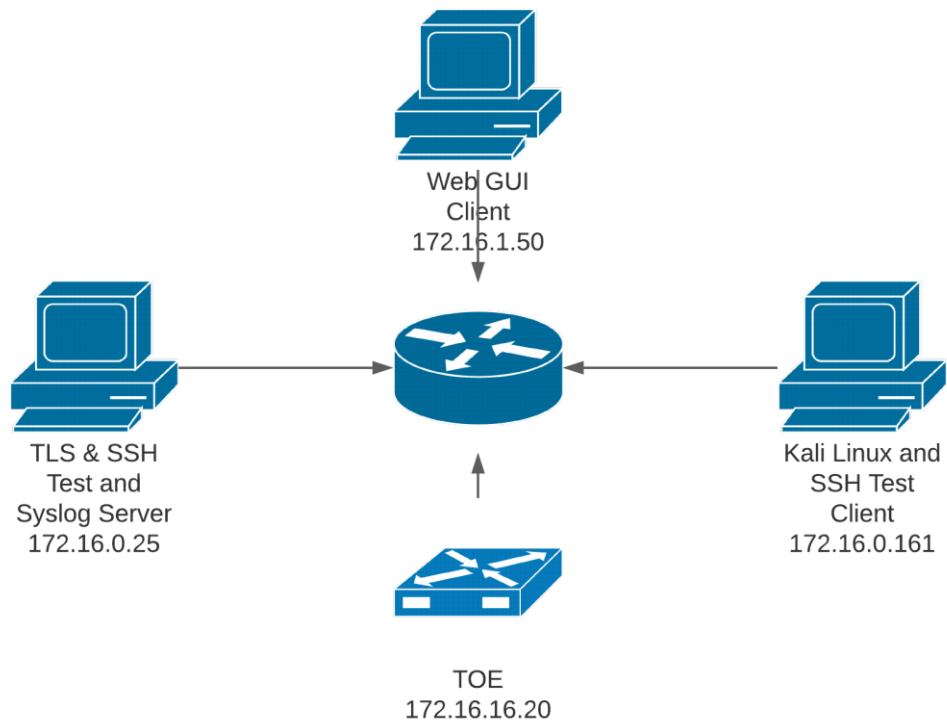
Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from September 2021 to February 2022.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

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

7.1 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration. The test configuration is shown below:

**TOE**

OneIdentity SPS Model 3000 running firmware version 6.9.4.

Web GUI Client

Microsoft Windows 2016 Server Datacenter

Google Chrome Version 97

Putty release 0.71

TLS Test and Syslog Server

Ubuntu 18.04

Wireshark 2.6.10

SSLyze 2.1.4

OpenSSL 1.1.1

Python

Leidos Proprietary TLS tools

Kali Linux and SSH Test Client

Kali Linux Release 2020.4

Wireshark 2.6.10

XCA Certificate Authority 2.0.1

SSLyze 2.1.4

Apache Web Server 2.4.4.1 (for CRL distribution)

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the hardware and software listed below when configured in accordance with the documentation specified in Section 6. The TOE consists of the following hardware components:

- Model 3000 with Intel Xeon E3-1275 CPU (Kaby Lake)
- Model 3500 with 2 x Intel Xeon Silver 4110 CPU (Skylake)

These hardware components include the One Identity Safeguard for Privileged Sessions 6.9 software/firmware, which runs on a modified version of Ubuntu Linux LTS 18.04 as its base operating system plus additional software/firmware needed to support the product's functionality. The software/firmware is obtained and installed as a single bundle that includes the underlying operating system; it is not installed as a separate application on a general-purpose server operating system.

Depending on configuration, the TOE in its evaluated configuration may require the following components in its operational environment:

- A TLS-protected syslog server that receives audit events from the TOE,
- A TLS-protected LDAP server used for remote administrator authentication, if configured
- Administrative workstation
- SSH clients/servers (for which the TOE acts as a session proxy between them)
- A client workstation for administrator access to the local console and web UI with:
 - A supported operating system: Windows 2008 Server, Windows 7, Windows 2012 Server, Windows 2012 R2 Server, Windows 8, Windows 8.1, Windows 10, Windows 2016, or any recent version of Linux. The OS must have the ability to run fairly recent web browser browser.
 - A supported browser: current version of Mozilla Firefox, current version of Google Chrome, Microsoft Edge, and Microsoft Internet Explorer 11 or newer. The browser must support TLS-encrypted HTTPS connections, and JavaScript/cookies must be enabled.
 - A physical interface that allows for serial port connectivity to the local console port.

8.2 Excluded Functionality

The list below identifies features or protocols that are not evaluated or must be disabled and the rationale why.

Feature	Description
Cluster and HA Deployments	Cluster and HA deployments were not evaluated.
Desktop Player Application	Excluded from the evaluation boundary since its functionality does not relate to the NDcPP requirements.
Privileged Analytics	Privileged Analytics is enabled for the evaluated configuration of the product but is outside the evaluation boundary since its functionality does not relate to the NDcPP requirements. Enabling

	this feature shows that it is “non-interfering” with respect to the product’s ability to meet the claimed security requirements
RADIUS	RADIUS must be disabled in the evaluated configuration because it does not use a cryptographic channel (e.g. RadSec).
Safeguard for Privileged Passwords (SPP)	Use of SPP for any purpose (i.e. user-initiated and SPS-initiated) is excluded. The channel must not be configured/used.
TLS break-and-inspect functionality (TLS/HTTPS proxy)	Excluded from the evaluated configuration since its functionality is not related to the NDcPP requirements.
SSH administrative access	Administrative access using SSH is disabled in the evaluated configuration.
Any features not associated with SFRs in [NDcPP]	NDcPP forbids adding additional requirements to the Security Target (ST). If additional functionalities or products are mentioned in the ST, it is for completeness only.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for One Identity Safeguard for Privileged Sessions 6.9. The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 and CEM version 3.1, revision 5, and the specific evaluation activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019*). The evaluation determined the TOE satisfies the conformance claims made in the One Identity Safeguard for Privileged Sessions 6.9 Security Target, of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in:

- *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020*.

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

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

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

9.2 Evaluation of the Development (ADV)

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

9.3 Evaluation of the Guidance Documents (AGD)

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

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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

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

9.6 Vulnerability Assessment Activity (AVA)

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

Searches of public vulnerability repositories were performed on 3 March 2022.

The evaluation team searched the following public vulnerability repositories.

- National Vulnerability Database (<http://web.nvd.nist.gov/view/vuln/search>)
- US-CERT Vulnerability Notes Database (<https://www.kb.cert.org/vuls/>)
- The vendor's notifications and alerts page for the product (<https://support.oneidentity.com/one-identity-safeguard-for-privileged-sessions/all/alerts-notifications>)
- Ubuntu Security Notices (for the Ubuntu 18.04 LTS operating system that the TOE relies on) (<https://ubuntu.com/security/notices?order=newest&release=bionic&details=>)
- Ubuntu CVEs (for the Ubuntu 18.04 LTS operating system that the TOE relies on) (<https://ubuntu.com/security/cves>)

The evaluation team used the following search terms in the searches of these repositories:

- one identity/one identity safeguard/safeguard for privileged sessions/balabit (product name, current developer, former developer)
- intel/xeon/kaby lake/skylake (processor make and model)
- sc113/superserver/1029u-t/supermicro (hardware chassis make and model)
- ubuntu 18.04 LTS (TOE base operating system)
- nginx (TOE web server)
- openssl (TOE TLS and general cryptographic engine)
- postgresql/rabbitmq/cherrypy/openldap/freerdp/log4j/syslog-ng/sudo/angular2 (significant third-party software components contained within the TOE software)
- (significant third-party software components contained within the TOE software)

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

9.7 Summary of Evaluation Results

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

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

10 Validator Comments/Recommendations

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

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

11 Security Target

The ST for this product's evaluation is *One Identity Safeguard for Privileged Sessions 6.9 Security Target, Version 1.0, 20 January 2022*.

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AD	Active Directory
AES	Advanced Encryption Standard
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
HTTP(S)	Hypertext Transfer Protocol (Secure)
LDAP	Lightweight Directory Access Protocol
OE	Operational Environment
OS	Operating System
SFR	Security Functional Requirement
SPS	Safeguard for Privileged Sessions (the TOE)
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

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

- [1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
- [2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- [3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.
- [4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.
- [5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.
- [6] Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019
- [7] One Identity Safeguard for Privileged Sessions 6.9 Security Target, Version 1.0, January 20, 2022
- [8] One Identity Safeguard for Privileged Sessions 6.9 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.1, January 26, 2022
- [9] One Identity Safeguard for Privileged Sessions 6.9.3 Installation Guide, April 30, 2021
- [10] One Identity Safeguard for Privileged Sessions 6.9.3 Packaging Checklist, April 30, 2021
- [11] One Identity Safeguard for Privileged Sessions 6.9.3 Upgrade Guide, April 30, 2021
- [12] One Identity Safeguard for Privileged Sessions 6.9.3 Administration Guide, April 30, 2021
- [13] One Identity Safeguard for Privileged Sessions 6.9.3 REST API Reference Guide, April 30, 2021
- [14] Super SC113 Chassis Series User's Manual, Version 1.0d, October 2, 2013
- [15] Supermicro SuperServer 1029U-T Series User's Manual, Revision 1.0i, September 22, 2020
- [16] One Identity Safeguard for Privileged Sessions 6.9.4 Release Notes, January 27, 2022
- [17] Supermicro BMC IPMI User's Guide, Revision 1.1b, August 26, 2020
- [18] Evaluation Technical Report for One Identity Safeguard for Privileged Sessions 6.9 (Leidos Proprietary), Version 1.0, 28 February 2022
- [19] Assurance Activities Report for One Identity Safeguard for Privileged Sessions 6.9, Version 1.0, 28 February 2022
- [20] One Identity Safeguard for Privileged Sessions 6.9 Common Criteria Test Report and Procedures (Leidos Proprietary), Version 1.1, February 28, 2022
- [21] (Leidos Proprietary) One Identity Safeguard for Privileged Sessions 6.9 Vulnerability Assessment, Version 1.1, February 22, 2022