

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

**CyberArk Privileged Access Security – Linux Components
including Privileged Session Manager SSH Proxy (PSMP)
v10.4 and On-Demand Privileges Manager (OPM) v10.4**

Report Number: CCEVS-VR-11006-2019

Dated: September 30, 2019

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

Marybeth Panock

Evaluation Team

Eve Pierre

Cheryl Dugan

Common Criteria Testing Laboratory

DXC

10830 Guilford Road, Suite 307

Annapolis Junction, Maryland 20701

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4, the Target of Evaluation (TOE), performed by DXC. It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by DXC of Annapolis Junction, MD in accordance with the United States evaluation scheme and completed on September 27, 2019. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012 at Evaluation Assurance Level 1, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012 – and the NIAP Protection Profile for Application Software v1.2; April 22, 2016.

CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4, the TOE, which contains the PSMP and OPM software, both of which run on a Linux operating system (OS). PSMP acts as a proxy for SSH-enabled devices by controlling access to privileged sessions and initiating SSH connections to remote devices on behalf of the user without the need to disclose SSH credentials

The OPM component is accessible via the OPM Client TSFI, and it allows users to obtain privileged account permissions and privileged command access from their local Linux session without obtaining the root credentials or super user access.

The Evaluation Team performed an analysis of the international interpretations of the CC, CEM and determined that none of the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before June 1, 2019.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

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 Validated Products List.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	CyberArk Software Ltd. (CyberArk) Privileged Access Security – Linux Components, including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4
Protection Profile	Protection Profile for Application Software v1.2; April 22, 2016
Security Target	CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 Security Target, version 0.17, September 27, 2019
Date of evaluation	September 30, 2019
Evaluation Technical Report	CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 Evaluation Technical Report, v0.4, September 27, 2019
Assurance Activity Report	Assurance Activity Report for CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4, v0.6, September 2019
Conformance Result	<ol style="list-style-type: none">1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012. <p>The following CC conformance:</p> <ul style="list-style-type: none">• Part 2 extended• Part 3 extended• Protection Profile for Application Software v1.2; April 22, 2016 conformant.
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012

Item	Identifier
Common Evaluation Methodology (CEM) version	CEM version 3.1R4, April 2017
Sponsor	CyberArk Software
Developer	CyberArk Software
Evaluators	Eve Pierre, Cheryl Dugan
Validation Team	Daniel Faigin, Marybeth Panock

3. SECURITY POLICY

The TOE is a software-only TOE and is comprised of the Privileged Session Manager SSH Proxy (PSMP) and on-Demand Privilege Manager (OPM) software, along with the Version Check Tool.

In the evaluated configuration, PSMP and OPM are installed on the RHEL 7.4 OS. All TOE components require access to the same internal network in which the EPV server is installed in order to interact with it. Note that the platform that the TOE is installed on will not be allowed to have access to the internet and is intended for only intranet use. PSMP will also be used to connect to remote targets using SSH to allow TOE users to securely interact with devices on the internal network.

Any data leakage across the TOE may cause severe damage to the organization and therefore must be prevented.

4. SECURITY PROBLEM DEFINITION

Assumptions

The ST identified the following security assumptions:

TABLE 1: TOE ASSUMPTIONS

Assumption Name	Assumption Definition
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

Threats

The ST identified the following threats addressed by the TOE:

TABLE 2: TOE THREATS

Threat Name	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

TABLE 3: ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies for the application.

5. ARCHITECTURAL INFORMATION

Physical Scope and Boundary

The TOE Boundary includes all the CyberArk developed parts of the PSMP and OPM products.

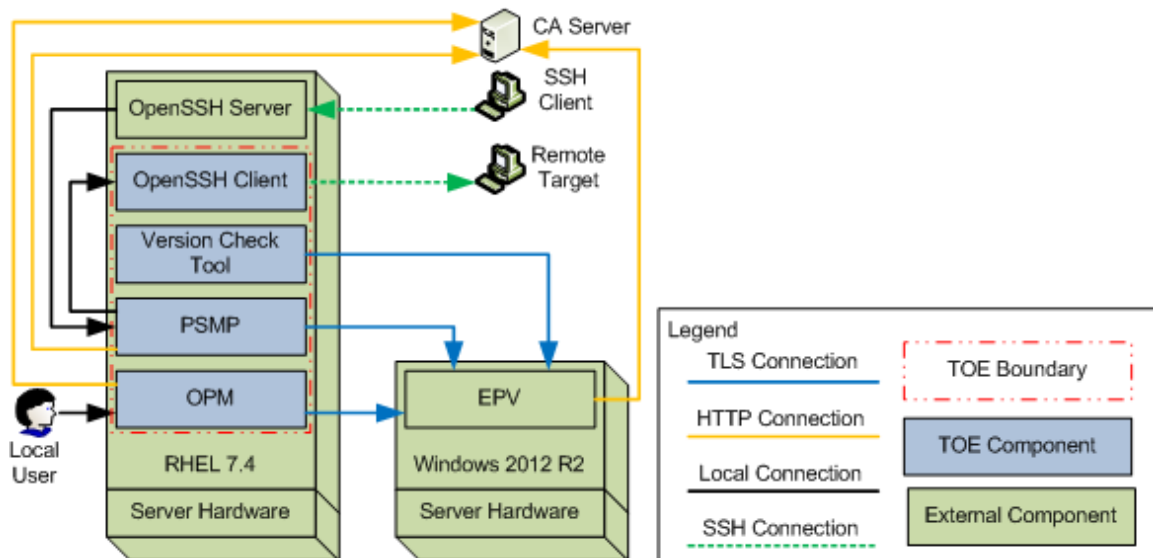


Figure 1 – Toe Boundary

The TOE is a software-only TOE and is comprised of the PSMP and OPM software. This TOE was evaluated as a single component consisting of multiple processes. It is *not* a distributed TOE. It is also not multiple products packaged together for evaluation structuring, where each product independently meets all SFRs. The two main Linux components, Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4, along with the Version Check tool, combined, meet the SFRs. SFRs were assessed against all components implementing the functionality, or subject to the threats, addressed by the indicated SFR.

Required TOE Components and Applications

For the evaluated configuration, the following TOE software must be installed on the RHEL machine in the environment:

- CyberArk PSMP v10.4.1-3.x86_64
 - Including PSMP's OpenSSH Client
- CyberArk OPM v10.04.01.2.x86_64
- CyberArk Version Check Tool

Logical Scope and Boundary

The logical scope of the TOE comprises the following security functions:

Cryptographic Support — The TOE uses CAVP-validated cryptographic algorithm provided by its own CyberArk cryptographic libraries. The library is used to support the establishment of trusted channels to protect data in transit. In the evaluated configuration, the TOE's cryptographic library is used by the OpenSSH Client to remote targets and the TLS client connection to the EPV server.

User Data Protection — The TOE stores sensitive information in the form of encrypted passwords in non-volatile memory. The TOE will limit its access to only network connectivity when accessing the platform's hardware resources. The network connection is used for communications between the TOE to the EPV server, the TOE to the target devices, and the user to the TOE. The TOE will also access the EPV server's sensitive information repository (safes) when it needs to authenticate users or request root credentials.

Identification and Authentication - To validate the EPV server's certificate during the TLS handshake, the TOE implements functionality to validate X.509 certificates. The TOE uses a CRL¹ to check certificate revocation status and will not establish a connection to the EPV server when the CRL is unavailable.

Security Management — The TOE is configured with default file permissions already in place and does not provide default credentials for user authentication. The TOE relies on the platform for storing and setting configuration options within its config files. Administrators are able to configure the basic PSMP or OPM configuration parameters and restart the related service.

Privacy — The TOE does not store or transmit any Personally Identifiable Information (PII).

Protection of the TSF — The TOE protects against exploitation by implementing address space layout randomization (ASLR) and not allocating memory with both writing and execution. The TOE is also compatible with SELinux and is compiled with stack-based buffer overflow protection. It also stores user-modifiable files to directories that do not contain executable files.

The TOE uses standard platform APIs² and includes only the third-party libraries it needs to perform its functionality.

The TOE version can be checked using commands provided by the platform. Checking for updates to the TOE is reliant on the platform's functionality. Any update downloaded for the TOE must be installed using the platform's package manager. An administrator will install a public key from CyberArk that is used by the package manager to verify the integrity of any updates to the TOE.

Trusted Path/Channel — The TOE provides a trusted channel between itself and target devices over SSH using OpenSSH Client. The SSH software used by the TOE follows the Extended Package for Secure Shell. A trusted TLS channel is used between itself and the EPV server.

¹ CRL – Certificate Revocation List

² API – Application Programming Interface

6. DOCUMENTATION

The TOE includes the following security target and guidance documents:

- CyberArk Software Ltd. Privileged Access Security – Linux Components Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4, version 0.17, September 27, 2019
- CyberArk: Privileged Access Security Installation Guide; Version 10.4; PASIN-10-4-0-1
- CyberArk: Privileged Access Security System Requirements; Version 10.4; PASSR-10-4-0-1
- CyberArk; Privileged Access Security End-user Guide; Version 10.4; PASEUG-10-4-0-1
- CyberArk; Privileged Access Security Reference Guide; Version 10.4; PASRG-10-4-0-1
- CyberArk; Privileged Access Security Implementation Guide; Version 10.4; PASIMPG-10-4-0-1
- CyberArk.; Privileged Access Security – Linux Components; Guidance Documentation Supplement; Document Version: 0.8

All documentation delivered with the product is relevant to and within the scope of the TOE.

7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

Evaluation team independent testing

The evaluation team conducted independent testing at the CyberArk facilities in Petach-Tikva, Israel. The evaluation team configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the Independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification. The vulnerability analysis was completed on August 28, 2019.

8. RESULTS OF THE EVALUATION

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

DXC has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Application Software v1.2; April 22, 2016. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on September 27, 2019.

9. VALIDATOR COMMENTS

As stated earlier in this report, the product is the CyberArk PAS Solution, which enables organizations to secure, provision, control, and monitor all activities associated with the privileged identities used in enterprise systems. PAS contains multiple applications that work together to provide privileged access security. However, the components of the PAS Solution were not evaluated as a distributed TOE but as standalone TOEs that work together. There are separate security targets, detailed test reports, assurance activity reports, and secure configure guidance supplement. This validation report covers the evaluation of the Linux components Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4.

The reader should review the Guidance Documentation Supplements and the associated guidance documents identified in section 6 carefully to ensure secure configuration of the product.

All other items and scope issues have been sufficiently addressed elsewhere in the document.

10. ANNEXES

None

11. SECURITY TARGET

CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 Security Target, version 0.17, September 27, 2019

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. Protection Profile for Application Software v1.2; April 22, 201
6. CyberArk Software Ltd. Privileged Access Security – Linux Components including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 Security Target, version 0.17, September 27, 2019
7. Assurance Activity Report for CyberArk Privileged Access Security – Linux Components including PSMP v10.4.1-3.x86_64 and OPM v10.04.01.2.x86_64, 0.6, September 2019
8. CyberArk Privileged Access Security – Linux Components including PSMP v10.4.1-3.x86_64 and OPM v10.04.01.2.x86_64 Evaluation Technical Report, v0.4, September 27, 2019
9. PAS-LINUX COMPONENTS Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 DETAILED TEST REPORT Document Version 0.5 September 27, 2019
10. CyberArk: Privileged Access Security Installation Guide; Version 10.4; PASIN-10-4-0-1
11. CyberArk: Privileged Access Security System Requirements; Version 10.4; PASSR-10-4-0-1
12. CyberArk; Privileged Access Security End-user Guide; Version 10.4; PASEUG-10-4-0-1
13. CyberArk; Privileged Access Security Reference Guide; Version 10.4; PASRG-10-4-0-1
14. CyberArk; Privileged Access Security Implementation Guide; Version 10.4; PASIMPG-10-4-0-1
15. CyberArk Software Ltd. Privileged Access Security – Linux Components; Guidance Documentation Supplement; Document Version: 0.8

