Product Compliance Listing Entry

Target of Evaluation: CyberArk Privilege Access Security – Linux Components Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4.

Product Technology Type: Application Software

Date of Certificate: September 30, 2019

Conformance Claim: Protection Profile Compliant

Protection Profile Identifier:

Protection Profile for Application Software, version 1.2, 04-22-2016

Extended Package for Secure Shell (SSH) v1.0

Vendor Contact Information:

Company Name: CyberArk Software Ltd

Vendor POC: Yariv Oren

Email: yariv.oren@cyberark.com

Phone: 972.3.918.0000

Web Address: www.cyberark.com

Vendor Logo:

CYBERARK

Common Criteria Testing Laboratory: DXC

PRODUCT DESCRIPTION:

CyberArk Privilege Access Security – Linux Components Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 is a software-based solution that runs on Linux and is a component of CyberArk's Privileged Access Security (PAS) Solution. PAS enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications. PSMP enables organizations to secure, control, and monitor privileged access to network devices. OPM enables organizations to secure, control, and monitor privileged access to UNIX commands by allowing end users to perform super-user tasks with their own personal account without the need to know super-user credentials.

SECURITY EVALUATION SUMMARY:

The evaluation was carried out in accordance to the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the product meets the security requirements contained in the Security Target. The criteria against which the CyberArk Privilege Access Security – Linux Components Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4. DXC determined that the product is conformant to requirements for Protection Profile for Application Software, version 1.2, 04-22-2016. The product satisfies all of the security functional requirements stated in the Security Target. Two validators, on behalf of the CCEVS Validation Body, monitored the evaluation carried out by DXC. The evaluation was completed in September 27, 2019. Results of the evaluation can be found in Assurance Activity Report for CyberArk Privilege Access Security – Linux Components Including Privileged Session Manager SSH Proxy (PSMP) v10.4 and On-Demand Privileges Manager (OPM) v10.4 prepared by DXC.

ENVIRONMENTAL STRENGTHS:

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

TOE implements 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 CRL 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.

Protection of the TSF The TOE protects against exploitation by implementing address space layout randomization (ASLR) except for vsyscall 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 APIs12 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 functionally. 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/Channels — 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.