Certification Report

CyberArk Privileged Account Security Solution v9.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-303-CR
Version: 1.0
Date: 29 June 2015
Pagination: i to iii, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 29 June 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

CyberArk Privileged Account Security Solution v9.1 (hereafter referred to as CyberArk PASS v9.1), from CyberArk Software, Ltd, is the Target of Evaluation(TOE). The results of this evaluation demonstrate that CyberArk PASS v9.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

CyberArk PASS v9.1 is software-based identity management solution for managing privileged accounts in the enterprise. The TOE is comprised of multiple standalone software and interfaces modules which enable organizations to secure, provision, control, and monitor all activities associated with enterprise systems and applications.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 29 June 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for CyberArk PASS v9.1, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the CyberArk PASS v9.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

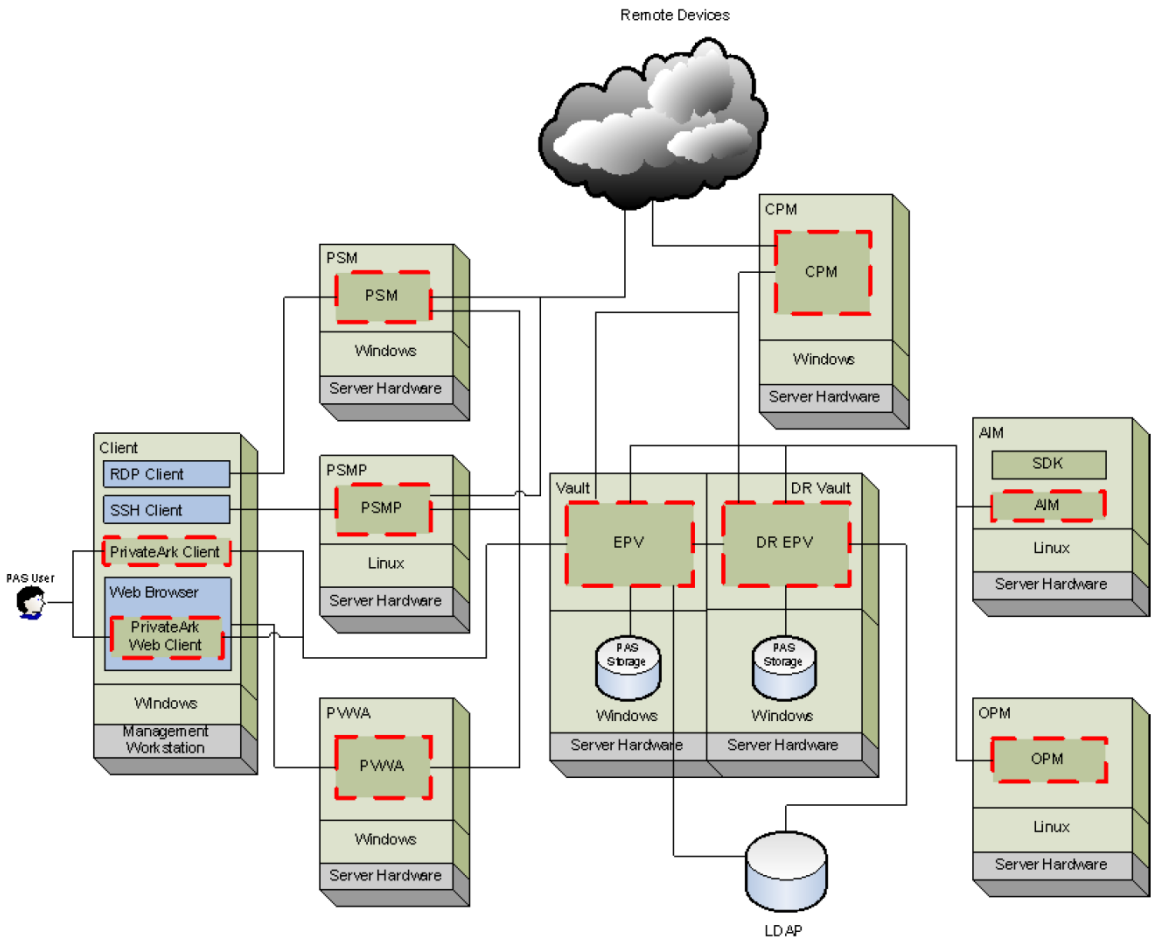
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is CyberArk Privileged Account Security Solution v9.1 (hereafter referred to as CyberArk PASS v9.1), from CyberArk Software, Ltd.

2 TOE Description

CyberArk PASS v9.1 is software-based identity management solution for managing privileged accounts in the enterprise. The TOE is comprised of multiple standalone software and interfaces modules which enable organizations to secure, provision, control, and monitor all activities associated with enterprise systems and applications.

A diagram of the CyberArk PASS v9.1 architecture is as follows:



3 Security Policy

CyberArk PASS v9.1 implements a role-based access control policy to control administrative access to the system. In addition, CyberArk PASS v9.1 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TSF*
- *Resource Utilization*
- *TOE Access*
- *Trusted Path/Channel*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
OpenSSL FIPS Object Module	*1051*
OpenSSL FIPS Object Module	*1747*

4 Security Target

The ST associated with this Certification Report is identified below:

CyberArk Software Privileged Account Security Solution v9.1 Security Target, 1.8, April 24, 2015

5 Common Criteria Conformance

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

CyberArk PASS v9.1 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following: ALC_FLR.2

b. Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

- FPT_APW_EXT Protection of Stored Credentials

c. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of CyberArk PASS v9.1 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *TOE Administrators are non-hostile and are trusted to follow and apply all administrator guidance.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.*
- *The TOE software will be protected from unauthorized modification.*
- *The IT environment provides the TOE with the necessary reliable timestamps.*
- *The EPV component of the TOE will be installed on a hardened instance of Windows*
- *Access to the TOE will be provided by a reliable network connection*
- *TOE components will be installed onto a compatible Operating System*
- *All LDAP and remote systems that the TOE communicates with should be located on the same internal network as the TOE.*

7 Evaluated Configuration

The evaluated configuration for CyberArk PASS v9.1 comprises:

The TOE components installed on servers and workstations with the following operating systems;

- Windows 2012 R2 - Hardened (EPV)
- Windows 2012 R2 (64-bit) (PSM, PVWA, CPM)
- Red Hat Enterprise Linux (RHEL) 5.3 (64-bit) (AIM, OPM, PSMP)
- Windows 7 Enterprise SP1 (PrivateArk Client)

The TOE also requires the following environmental components;

- MS Active Directory

The publication entitled CyberArk Privileged Account Security Solution v9.1 Guidance Supplement, 0.6, 29 May 2015 describes the procedures necessary to install and operate CyberArk PASS v9.1 in its evaluated configuration.

8 Documentation

The CyberArk Software, Ltd documents provided to the consumer are as follows:

a. Central Credential Provider Implementation Guide, 9.0.0

b. Privileged Account Security Installation Guide, 9.1

c. Privileged Account Security Reference Guide, 9.1

d. Privileged Account Security System Requirements, 9.1

e. Privileged Account Security End-user Guide, 9.1; and

f. Privileged Account Security Release Notes, 9.1

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of CyberArk PASS v9.1, including the following areas:

Development: The evaluators analyzed the CyberArk PASS v9.1 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the CyberArk PASS v9.1 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the CyberArk PASS v9.1 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the CyberArk PASS v9.1 configuration management system and associated documentation was performed. The evaluators found that the CyberArk PASS v9.1 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of CyberArk PASS v9.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the CyberArk PASS v9.1. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[1].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Audit Generation: The objective of this test goal is to confirm the generation of audit records and that they cannot be deleted;

c. User Data protection: The objectives of this test goal are to confirm that communication between separate parts of the TOE is protected, that session timeouts occur, and that session establishment can be denied based upon time; and

d. Authentication Mechanism Bypass: The objective of this test goal is to confirm that the authentication mechanisms in place cannot be bypassed in a trivial manner.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities; and

b. Scanning for HEARTBLEED, POODLE, GHOST, FREAK, SHELLSHOCK.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

10.4 Conduct of Testing

CyberArk PASS v9.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that CyberArk PASS v9.1 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AIM	Application Identity Manager
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CPM	Central Policy Manager
EAL	Evaluation Assurance Level
EPV	Enterprise Password Vault
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OPM	On-demand Privileges Manager
PALCAN	Program for the Accreditation of Laboratories - Canada
PSM	Privileged Session Manager
PSMP	Privileged Session Manager SSH Proxy
PVWA	Password Vault Web Access
SDK	Software Development Kit
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. CyberArk Software Privileged Account Security Solution v9.1 Security Target, 1.8, April 24, 2015

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of CyberArk Software, Ltd Privileged Account Security Solution v9.1 Document No. 1862-000-D002 Version 0.3, 29 June 2015.