National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, 06 December 2019

Report Number: CCEVS-VR-PP-0066
Dated: 28 January 2021
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6982
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory
Base Requirements
CGI IT Security Labs
Fairfax, Virginia

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0 (EP_SV_V1.0), which is intended for use with the Protection Profile for Virtualization (PP_BASE_VIRTUALIZATION_V1.0) Base-PP. It presents a summary of the EP_SV_V1.0 and the evaluation results.

CGI IT Security Labs, located in Fairfax, Virginia, performed the evaluation of the EP_SV_V1.0 concurrent with the first product evaluation against the Extended Package (EP) requirements. The evaluated product was VMware ESXi 6.7 Update 2. This evaluation addressed the single base requirement of EP_SV_V1.0.

The Validation Report (VR) author independently performed an additional review of the EP as part of the completion of this VR, to confirm it meets the claimed APE requirements. The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements. During the evaluation, it was determined that the EP was missing the SFR Rationale. NIAP issued a Technical Decision to update add an SFR Rationale. After further review, it was verified that these issues resolved all PP deficiencies and had no impact on the product evaluation.

The evaluation determined the EP_SV_V1.0 is both Common Criteria Part 2 extended and Part 3 extended. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the EP identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from the EP_SV_V1.0; completion of the ASE work units satisfied the APE work units for this EP, but only for the materials defined in this EP.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and EPs that have Assurance Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 work units specific to the technology described by the PP or EP.

In order to promote thoroughness and efficiency, the evaluation of the EP_SV_V1.0 was performed concurrent with the first product evaluation against the EP's requirements. In this case, the Target of Evaluation (TOE) was VMware ESXi 6.7 Update 2, performed by CGI IT Security Labs in Fairfax, Virginia, United States of America.

The EP_SV_V1.0 has a set of base requirements all conformant STs must include.

The following identifies the EP evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this EP.

Extended Package	Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, 17 November 2016
ST (Base)	VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, 05 November 2019
Assurance Activity Report (Base)	Assurance Activities Report VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, Version 0.5, 05 November 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	CGI IT Security Labs 12601 Fair Lakes Circle Fairfax, VA 22033

3 EP_SV_V1.0 Description

The EP_SV_V1.0 along with the PP_BASE_VIRTUALIZATION_V1.0 provide a baseline set of Security Functional Requirements (SFRs) for virtualization systems that specifically implement Server Virtualization.

Server Virtualizations are virtualization systems that implement virtualized hardware components on server-class hardware. It creates a virtualized hardware environment for each instance of an operating system (virtual machines or VMs) permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. Each VM instance supports applications such as file servers, web servers, and mail servers. Server virtualization may also support client operating systems in a virtual desktop or thin-client environment. Typically, virtualized servers provide services to remote clients and are generally not directly accessible by non-administrative users.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows applicable assumptions the EP extends, in addition to those defined in the Base-PP.

Table 1: Assumptions

Assumption Name	Assumption Definition
This EP does not define any assumptions.	

4.2 Threats

Table 2 shows applicable threats the EP extends, in addition to those defined in the Base-PP. Note however that the SFR defined in this EP will assist in the mitigation of the T.UNAUTHORIZED_UPDATE and T.UNAUTHORIZED_ACCESS threats defined in that PP.

Table 2: Threats

Threat Name	Threat Definition
This EP does not define any threats.	

4.3 Organizational Security Policies

Table 3 shows applicable organizational security policies the EP extends, in addition to those defined in the Base-PPs.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
This EP does not define any organizational security policies.	

4.4 Security Objectives

Table 4 shows security objectives for the TOE the EP extends, in addition to those defined in the Base-PP. Note however that the SFRs defined in this EP will assist in the enforcement of the O.VMM_INTEGRITY and O.MANAGEMENT_ACCESS objectives defined in that PP.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
This EP does not define any security objectives for the TOE.	

Table 5 shows security objectives for the Operational Environment, in addition to those defined in the Base-PP.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
This EP does not define any security objectives for the operational environment.	

5 Requirements

As indicated above, the EP_SV_V1.0 requirement includes one base mandatory requirement. Table 6 shows the mandatory requirement validated as part of the VMware ESXi 6.7 Update 2 evaluation activities referenced above.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	VMware ESXi 6.7 Update 2

6 Assurance Requirements

As an EP of the Base Virtualization PP, this EP does not prescribe any SARs beyond those defined in the base PP. The SARs defined in the base PP are applicable to the EP_SV_V1.0.

7 Results of the Evaluation

Note that for APE elements and work units identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 7: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_INT.1	Pass	VMware ESXi 6.7 Update 2
APE_CCL.1	Pass	VMware ESXi 6.7 Update 2
APE_SPD.1	Pass	VMware ESXi 6.7 Update 2
APE_OBJ.1	Pass	VMware ESXi 6.7 Update 2
APE_ECD.1	Pass	VMware ESXi 6.7 Update 2
APE_REQ.1	Pass	VMware ESXi 6.7 Update 2

8 Glossary

The following definitions are used throughout this document:

- **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.
- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the EP_SV_V1.0 Assurance Activities to determine whether the claims made are justified.
- **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.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance 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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Protection Profile for Virtualization Extended Package Server Virtualization, Version 1.0, 17 November 2016.

[7] Protection Profile for Virtualization, Version 1.0, 17 November 2016.

[8] VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, 05 November 2019.

[9] Assurance Activities Report VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, Version 0.5, 05 November 2019.