National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

VMware ESXi 6.7 Update 2

Report Number: CCEVS-VR-VID10964-2019
Dated: November 11, 2019
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

John Butterworth
Michelle S Carlson,
Patrick W Mallet, PhD
Lisa Mitchel
Clare Olin
MITRE Corporation

Jerome F Myers, PhD
Aerospace Corporation

Common Criteria Testing Laboratory

Swapna Katikaneni
Madelyn Lanoue
CGI IT Security Labs

Table of Contents

List of Tables

1 Executive Summary

This report 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 Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of VMware ESXi 6.7 Update 2 (hereafter referenced as VMware ESXi). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of VMware ESXi was performed by CGI IT Security Labs in Fairfax, Virginia, in the United States and was completed in November 2019. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 5 and assurance activities specified in Protection Profile for Virtualization Version 1.0 with the Extended Package Server Virtualization Version 1.0 and Extended Package for Secure Shell (SSH) Version 1.0. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The CGI Information Technology Security Lab (ITSL) evaluation team determined that VMware ESXi is conformant to the claimed Protection Profile (PP) and EP's. The TOE when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST.

The VMware ESXi TOE is designed to act as a virtualization platform, providing the ability to implement and virtualize different workloads across multiple virtual machines (VMs). The TOE is a software-only TOE and is installed on a platform consisting of a Dell PowerEdge R740 server with Intel Xeon 6126 "Skylake" CPUs.

Only the Hypervisor constitutes the TOE. The physical hardware platform and any VMs are not part of the TOE. Figure 1 shows the relationship between the TOE boundary and other components.

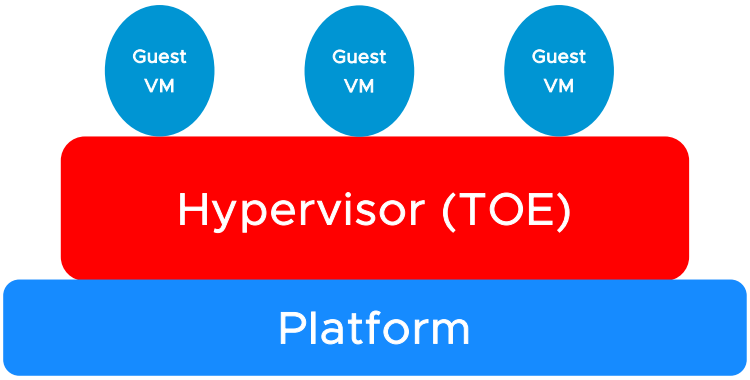

Figure 1: TOE Boundary

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP and EP's had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001
PP	Protection Profile for Virtualization Version 1.0 with the Extended Package Server Virtualization Version 1.0 and Extended Package for Secure Shell (SSH) Version 1.0.
ST	VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, November 5, 2019
ETR	Evaluation Technical Report for VMware ESXi 6.7 Update 2, Version 1.1, November 6, 2019
Sponsor & Developer	3401 Hillview Ave Palo Alto, CA 94304 United States of America
CCTL	CGI IT Security Labs 12601 Fair lakes Circle Fairfax, VA 22033
Completion Date	October 2019
CC	Common Criteria Version 3.1 Revision 5, April 2017

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
Disclaimer	The information contained in this Validation Report is not an endorsement of the VMware ESXi 6.7 Update 2 by any agency of the U.S. Government and no warranty is either expressed or implied.
Evaluation Personnel	Swapna Katikaneni Madelyn Lanoue
Validation Personnel	John Butterworth, Clare Olin, Lisa Mitchel, Michelle S Carlson, Jerome Myers and Patrick Mallett

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 Common Criteria Testing Laboratories (CCTLs) 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 information technology 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).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001
ST Version	1.12
Publication Date	November 5, 2019
Vendor and ST Author	VMware, Inc.
TOE Reference	VMware ESXi 6.7 Update 2
Hardware Platform	Dell PowerEdge R740 server with Intel Xeon 6126 "Skylake" CPUs
TOE Software Version	VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001
Keywords	Virtualization

3 Architectural Information

The TOE is designed to act as a virtualization platform, providing the ability to implement and virtualize different workloads across multiple virtual machines (VMs). The TOE is a software-only TOE where the core component is installed directly on the bare metal hardware. The following figure provides a visual depiction of TOE External Interfaces and Components.

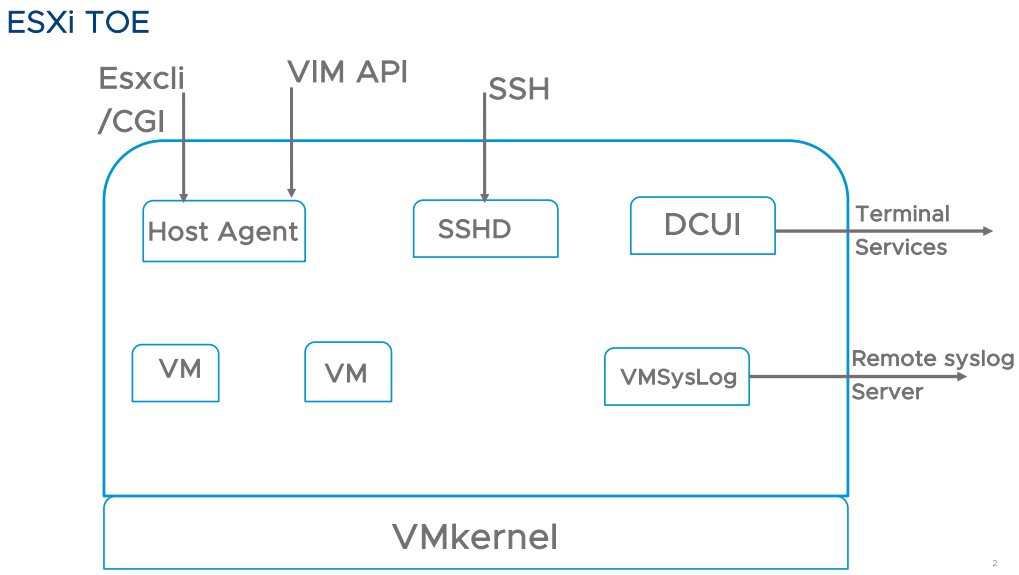

Figure 2: TOE External Interfaces and Components

4 Assumptions, Threats, and Scope

4.1 Assumptions

The ST identifies the following assumptions about the use of the product:

Table 3: Assumptions

Assumption	Description
A.PLATFORM_INTEGRITY	The platform has not been compromised prior to installation of the Virtualization System.
A.PHYSICAL	Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance.
A.COVERT_CHANNELS	If the TOE has covert storage or timing channels, then for all VMs executing on that TOE, it is assumed that relative to the IT assets to which they have access, those VMs will have assurance sufficient to outweigh the risk that they will violate the security policy of the TOE by using those covert channels.
A.NON_MALICIOUS_USER	The user of the VS is not willfully negligent or hostile, and uses the VS in compliance with the applied enterprise security policy and guidance. At the same time, malicious applications could act as the user, so requirements which confine malicious applications are still in scope.

4.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

Table 4: Threats

Threat	Description
T.DATA_LEAKAGE	It is a fundamental property of VMs that the domains encapsulated by different VMs remain separate unless data sharing is permitted by policy. For this reason, all Virtualization Systems shall support a policy that prohibits information transfer between VMs. It shall be possible to configure VMs such that data cannot be moved between domains from VM to VM, or through virtual or physical network components under the control of the VS. When VMs are configured as such, it shall not be possible for data to leak between domains, neither by the express efforts of software or users of a VM, nor because of vulnerabilities or errors in the implementation of the VMM or other VS components.

Threat	Description
	If it is possible for data to leak between domains when prohibited by policy, then an adversary on one domain or network can obtain data from another domain. Such cross-domain data leakage can, for example, cause classified information, corporate proprietary information, or personally identifiable information to be made accessible to unauthorized entities.
T.UNAUTHORIZED_UPDATE	It is common for attackers to target outdated versions of software containing known flaws. This means it is extremely important to update Virtualization System software as soon as possible when updates are available. But the source of the updates and the updates themselves must be trusted. If an attacker can write their own update containing malicious code they can take control of the VS.
T.UNAUTHORIZED_MODIFICATION	System integrity is a core security objective for Virtualization Systems. To achieve system integrity, the integrity of each VMM component must be established and maintained. Malware running on the platform must not be able to undetectably modify Virtualization System components while the system is running or at rest. Likewise, malicious code running within a virtual machine must not be able to modify Virtualization System components.
T.USER_ERROR	If a Virtualization System is capable of simultaneously displaying VMs of different domains to the same user at the same time, there is always the chance that the user will become confused and unintentionally leak information between domains. This is especially likely if VMs belonging to different domains are indistinguishable. Malicious code may also attempt to interfere with the user's ability to distinguish between domains. The VS must take measures to minimize the likelihood of such confusion.
T.3P_SOFTWARE	In some VS implementations, critical functions are by necessity performed by software not produced by the virtualization vendor. Such software may include Host Operating Systems and physical device drivers. Vulnerabilities in this software can be exploited by an adversary and result in VMM compromise. Where possible, the VS should mitigate the results of potential vulnerabilities or malicious content in third-party code.
T.VMM_COMPROMISE	The Virtualization System is designed to provide the appearance of exclusivity to the VMs and is designed to separate or isolate their functions except where specifically shared. Failure of security mechanisms could lead to unauthorized intrusion into or modification of the VMM, or bypass of the VMM altogether. This must be prevented to avoid compromising the Virtualization System.
T.PLATFORM_COMPROMISE	The VS must be capable of protecting the platform from threats that originate within VMs and operational networks connected to the VS. The hosting of untrusted—even malicious—domains by the VS cannot be permitted to compromise the security and integrity of the platform on which the VS executes. If an attacker can access the underlying platform in a manner not controlled by the VMM, the attacker might be able to modify system firmware or software—compromising both the Virtualization

Threat	Description
	System and the underlying platform.
T.UNAUTHORIZED_ACCESS	Functions performed by the management layer include VM configuration, virtualized network configuration, allocation of physical resources, and reporting. Only certain authorized system users (administrators) are allowed to exercise management functions. Virtualization Systems are often managed remotely over communication networks. Members of these networks can be both geographically and logically separated from each other, and pass through a variety of other systems which may be under the control of an adversary, and offer the opportunity for communications to be compromised. An adversary with access to an open management network could inject commands into the management infrastructure. This would provide an adversary with administrator privilege on the platform, and administrative control over the VMs and virtual network connections. The adversary could also gain access to the management network by hijacking the management network channel.
T.WEAK_CRYPTO	To the extent that VMs appear isolated within the Virtualization System, a threat of weak cryptography may arise if the VMM does not provide good entropy to support security-related features that depend on entropy to implement cryptographic algorithms. For example, a random number generator keeps an estimate of the number of bits of noise in the entropy pool. From this entropy pool random numbers are created. Good random numbers are essential to implementing strong cryptography. Cryptography implemented using poor random numbers can be defeated by a sophisticated adversary.
T.UNPATCHED_SOFTWARE	Vulnerabilities in outdated or unpatched software can be exploited by adversaries to compromise the Virtualization System or platform.
T.MISCONFIGURATION	The Virtualization System may be misconfigured, which could impact its functioning and security. This misconfiguration could be due to an administrative error or the use of faulty configuration data.
T.DENIAL_OF_SERVICE	A VM may block others from system resources (e.g., system memory, persistent storage, and processing time) via a resource exhaustion attack.

4.3 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and EP's and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.

3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation. In particular, the following ESXi features are excluded from the scope of this evaluation:
    - NSX software
    - vSAN software
    - VMware PowerCLI Software
    - vCenter Server software
    - vMotion
    - IPSec
    - Active Directory integration
    - 3rd Party VIBs (distributed independently of VMware ESXi)
    - VM Virtual Disk sharing
    - PCI passthrough (including vGPU)
    - SCSI passthrough
    - Raw disks
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not 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.

5 Security Policy

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

5.1 Security Audit

The ESXi security audit function collects and stores audit records in pre-allocated flat files on ESXi. Each audit record contains the:

- date and time of the event
- type of event
- subject identity
- object identity
- result (success or failure) of the event

ESXi provides a command to review its audit records. Reviewing the audit records on ESXi is restricted to administrators. ESXI also supports sending audit records to a collector external to the TOE.

5.2 Cryptographic Support

The TOE protects communications with components external to the TOE. It implements CAVP-validated cryptographic algorithms to handle all cryptographic functions to protect communications.
All passwords are hashed by the TOE. Cryptographic keys and other critical security parameters are never exposed in plain text. Certificates may only be imported through cryptographically validated channels.
The ESXi entropy subsystem is NIST sp 800-90A compliant.
Finally, VMs are provided access to a hardware entropy source for random bit generation.

5.3 User Data Protection

ESXi constrains direct access to all physical resources (CPU, memory, HDD, USB, etc.). VM data sharing is provided via virtual networks. Network traffic over a virtual network is only visible to the VMs configured for that virtual network.
VM access to USB physical devices as well as virtual networks is controlled by Administrators. Additionally, all volatile and non-volatile memory is zeroed to prevent residual data leakage.

5.4 Trusted Path/Channels

TOE remote communications are protected by CAVP-validated crypto primitives through SSH and TLS 1.2.

5.5 Identification and Authentication

Credentials (i.e. SSH public key, username/password) are required for an Administrator to gain access to ESXi. If the authentication credentials are valid, access to the system is provided. Failed and successful user login events are captured in the audit logs. The TOE also supports account lockout after a sufficient number of failed login attempts.
Password complexity policy is managed using standard PAM mechanisms.

The TOE uses X.509 certificate authentication for establishing trusted TLSv1.2 communication channels. ESXi performs validation of certificates through examination of the certificate path, CA flags, and extendedKeyUsage, as well as revocation checks against a CRL.

5.6 Security Management

Security management specifies how ESXi manages several aspects of the TSF, including TSF data and security functions. TSF data includes configuration data of the TOE, audit data, and system data.
The TOE supports remote administration over secure channels.
From a management perspective, access to ESXi objects is controlled via a role based access control mechanism. Only administrators can modify the access controls. For the purpose of this evaluation, the only role is Administrator. Thus all management functions are restricted to administrators.

5.7 TOE Access

The TOE displays an advisory warning message regarding unauthorized use of the TOE before establishing an Administrator session.

5.8 Protection of the TSF

The TSF is protected by the following mechanisms:

- Address space randomization,
- Memory execution protection (e.g., DEP)
- Stack buffer overflow protection
- Intel VT-x with EPT hardware assists

Protection of the TOE from physical tampering must be ensured by its environment. The TOE protects the confidentiality and integrity of all data as it is transmitted to and from the TOE.
For VMs, the TSF allows administrators to disable hypercalls to reduce the potential attack surface.
Lastly, the TSF provides administrators with the ability to manually update the TOE software with authenticated updates.

6 Documentation

VMware ESXi offers a number of guidance documents along with a CC-specific supplemental guidance document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Guidance Supplement version 1.16

This document in turn references the following documents that provide additional detailed guidance for specific TOE capabilities. Note that the evaluation examined these referenced documents only to the extent necessary to complete the assurance activities specified in the claimed PPs.

- VMware ESXi Installation and Setup, Published 11 APR 2019
- VMware ESXi Upgrade, Published 11 APR 2019
- vSphere Security, Published 11 APR 2019
- vSphere Single Host Management – VMware Host Client, Published 11 APR 2019
- vSphere Virtual Machine Administration, Published 11 APR 2019
- Guidance Supplement for VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001
  - (included in evaluation package)

This evaluation occurred with the versions of documentation listed above. The latest documents, which may be updated for releases following this evaluation, are maintained on the VMware documentation portal.

- https://docs.vmware.com/en/VMware-vSphere/index.html

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target Version 1.12, November 5, 2019

7 Independent Testing

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

- Independent Test Plan and Report for VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, Version 0.7, October 17,2019

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, Version 0.5, November 5, 2019

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to Protection Profile for Virtualization Version 1.0 with the Extended Package Server Virtualization Version 1.0 and Extended Package for Secure Shell (SSH) Version 1.0. Independent testing took place at the CGI ITSL location in Fairfax, Virginia.

Figure 3 below depicts a diagram of the test environment with a list of tools used by the evaluators. The Network Components and Software are shown in Table 7, following.

Figure 3: TOE Environment Setup

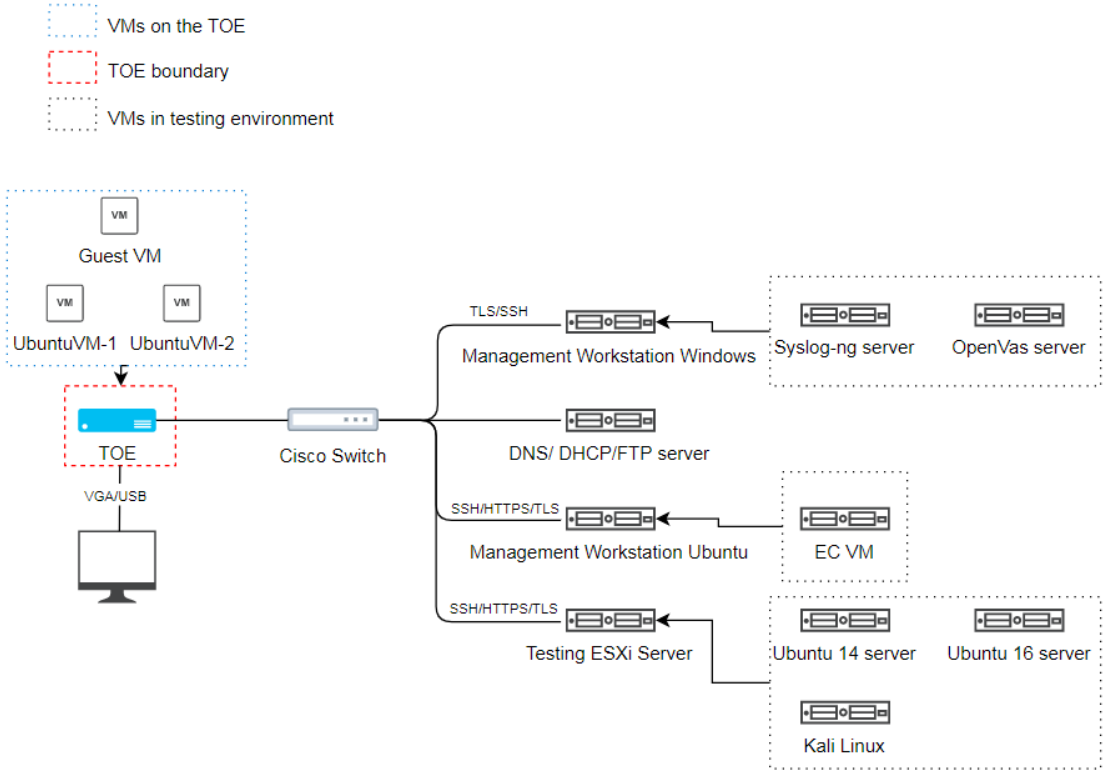

Table 5: Test Configuration Components and Tools Information

Test Network Component	Software	IP address
Cisco Catalyst Switch 3750X	Cisco IOS 15.0(2) SE4	172.16.11.1
Syslog-ng Server	syslog-ng 3.11.1	172.16.11.20
Ubuntu 14 server, OpenSSH Server	OpenSSH-6.9p1	172.16.11.11
Ubuntu 16 server, OpenSSL Server	OpenSSL-1.1.0d	172.16.11.10
Kali	Ettercap	172.16.11.9
OpenVas, Kali 2019.2	Nmap, OpenVas	DHCP
DNS Server		172.16.11.6
Management Workstation Ubuntu, CA Server	Wireshark, OpenSSL-1.1.0g, VMware Workstation	172.16.11.7
Management Workstation Windows	Virtual Box, vSphere	172.16.11.5
EC VM	Wireshark, OpenSSL-1.1.0g, ESXCLI, Vender provided Testing Script	172.16.11.12
Guest VM		DHCP
Ubuntu VM 1		DHCP
Ubuntu VM 2		DHCP

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the Protection Profile for Virtualization Version 1.0 with the Extended Package Server Virtualization Version 1.0 and Extended Package for Secure Shell (SSH) Version 1.0 have been fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE is VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001, as installed and configured according to the CC Configuration Guide as well as the supporting guidance documentation identified in Table 6.

The TOE evaluated configuration requires the following components shown in Table 8 below.

Table 6: Required IT Environment Components

Components	Description
Linux system for management	System from which to make VIM API calls or ESXCLI calls to configure and manage ESXi. *Any Linux distribution released after around 2014 should be sufficient. RHEL7 and Ubuntu 16.04 have been specifically tested.* *NOTE: In many deployments, vCenter Server is used to make VIM API calls.*
Remote Syslog Server	A server which implements RFC 3164 "The BSD Syslog Protocol" and RFC 5425 "TLS Transport Mapping for Syslog." *NOTE: A remote syslog server is optional. However, usage of a remote syslog server is included in the NIAP-validated configuration.*

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Virtualization Version 1.0 with the Extended Package Server Virtualization Version 1.0 and Extended Package for Secure Shell (SSH) Version 1.0, in conjunction with version 3.1, revision 5 of the CC and the CEM.

Examinations were performed on the Security Target, Development documentation, Test Documentation, and Guidance documentation. The validation team also performed an assessment on the evaluation lab's Assurance Activities Report.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the CGI ITSL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the VMware ESXi product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the PP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the PP and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the proprietary Penetration Test Report prepared by the evaluator, and summarized in the AAR. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols and TOE software version to ensure sufficient coverage under AVA. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The search was performed from August 12th 2019 to October 18th 2019. The search was updated on November 6th 2019.

The evaluator studied the following public vulnerability databases:

- United States Computer Emergency Readiness Team (US-CERT): https://www.kb.cert.org/vuls/search/
- Security Focus Vulnerability Database: https://www.securityfocus.com/vulnerabilities
- National Institute of Standards and Technology National Vulnerability Database (NVD): http://nvd.nist.gov/
- Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/cve/search_cve_list.html
- VMware Security Advisories : https://www.vmware.com/security/advisories.html

The following keywords were used for public searches:

- VMware ESXi 6.7 Update 2
- VMware ESXi 6.7
- VMware ESXi 6.7 Patch Release ESXi670-201905001
- Dell PowerEdge R740 server
- VMware TLS 1.2
- VMware SSH v2
- ESXi Direct Console User Interface
- VMware DCUI
- VMware Host Client

- VMware CGI API
- VMware VIM API
- VMware ESXCLI
- VMware OpenSSL FIPS Object Module version 2.0.20-vmw
- VMware VMKernel Cryptographic Module Loader v1.0
- vmkdrbg module

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the VMware ESXi that are outside the scope of the evaluation, PP's and EP's claimed and are not covered by this evaluation, need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, November 5, 2019

13 Abbreviations and Acronyms

Acronym	Definition
ADOM	Administrative Domain
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CSP	Critical Security Parameters
DRBG	Deterministic Random Bit Generator
FCoE	Fibre Channel over Ethernet
FIPS	Federal Information Processing Standard
iSCSI	Internet Small Computer System Interface
LDAP	Lightweight Directory Access Protocol
NDPP	Network Device Protection Profile
NFS	Network File Share
NTP	Network Time Protocol
OSP	Organizational Security Policy
PP	Protection Profile
PSC	Platform Services Controller
RAID	Redundant Array of Inexpensive Disks
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SCSI	Small Computer System Interface
SFP	Small Form-Factory Pluggable
SFR	Security Functional Requirement
SSO	Single Sign-On

ST	Security Target
TLB	Translation Lookaside Buffer
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
vCS	vCenter Server
vCSA	vCenter Server Appliance
VDOM	Virtual Domain
VM	Virtual Machine
VMDK	Virtual Machine Disk
VMM	Virtual Machine Manager
VPP	Virtualization Protection Profile

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

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

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Security Target, Version 1.12, November 5, 2019

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report for VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Version 1.1, November 6, 2019

[8] Assurance Activities Report for VMware ESXi 6.7 Update 2 with 6.7 Patch Version 201905001 Version 0.5, November 5, 2019