National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

VMware ESXi 7.0 Update 3d

Report Number: CCEVS-VR-VID11249-2022
Dated: 09/06/2022
Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Jim Donndelinger
Swapna Katikaneni
The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Contents

1 Executive Summary 1
2 Identification 2
3 TOE Architecture 4
4 Security Policy 6
4.1 Security Audit 6
4.2 Cryptographic Support 6
4.3 User Data Protection 6
4.4 Identification and Authentication 6
4.5 Security Management 6
4.6 Protection of the TSF 7
4.7 TOE Access 7
4.8 Trusted Path/Channels 7
5 Assumptions and Clarification of Scope 8
5.1 Assumptions 8
5.2 Clarification of Scope 8
6 Documentation 9
7 IT Product Testing 10
7.1 Test Configuration 10
8 TOE Evaluated Configuration 11
8.1 Evaluated Configuration 11
8.2 Excluded Functionality 11
9 Results of the Evaluation 12
9.1 Evaluation of the Security Target (ST) (ASE) 12
9.2 Evaluation of the Development (ADV) 12
9.3 Evaluation of the Guidance Documents (AGD) 12
9.4 Evaluation of the Life Cycle Support Activities (ALC) 13
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 13
9.6 Vulnerability Assessment Activity (AVA) 13
9.7 Summary of Evaluation Results 13
10 Validator Comments/Recommendations 14
11 Security Target 15
12 Abbreviations and Acronyms 16
13 Bibliography 17

List of Tables

Table 1: Evaluation Identifiers 2

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of VMware ESXi 7.0 Update 3d (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR 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 VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the *Protection Profile for Virtualization*, Version 1.1, 14 June 2021 ([5]), *PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021 ([6]), and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([8]).

The TOE is VMware ESXi 7.0 Update 3d.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found the evaluation demonstrated the product satisfies all of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) specified in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed PP and, when installed, configured and operated as described in the evaluated guidance documentation, satisfies all the SFRs specified in the ST ([9]).

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) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 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 Product Compliant List (PCL).

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

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware ESXi 7.0 Update 3d
Security Target	VMware ESXi 7.0 Update 3d Security Target, Version 1.0, 22 July 2022
Sponsor & Developer	VMware, Inc. 3401 Hillview Avenue Palo Alto, CA 94304
Completion Date	August 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	*PP-Configuration for Virtualization and Server Virtualization Systems*, Version 1.0, 4 June 2021, which contains the following: • *Protection Profile for Virtualization*, Version 1.1, 14 June 2021 • *PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021 • *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Pascal Patin
Validation Personnel	Jim Donndelinger Swapna Katikaneni

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE is VMware ESXi 7.0 Update 3d, installed on a Dell PowerEdge R740 server platform with Intel Xeon 6230R “Cascade Lake” CPUs.

VMware ESXi 7.0 Update 3d is a Type 1 (or “bare-metal”) hypervisor that is installed onto a computer system with no host platform OS and serves as a virtual machine manager (VMM) and virtualization system. This allows for the instantiation of multiple virtual machines (VMs) onto a single physical platform. It also implements mechanisms to enforce logical separation of VMs from one another and from the hypervisor so that data transmission between these domains can only occur through authorized interfaces.

The TOE consists solely of the VMware ESXi 7.0 Update 3d hypervisor—the hardware platform on which it is evaluated provides the operational environment for the TOE.

As a Type 1 hypervisor, the TOE consists of software/firmware components that are installed directly onto a physical platform without an intermediary operating system. Figure 1 shows the relationship between the TOE boundary and other components. Figure 2 shows the external interfaces and internal components of the TOE.

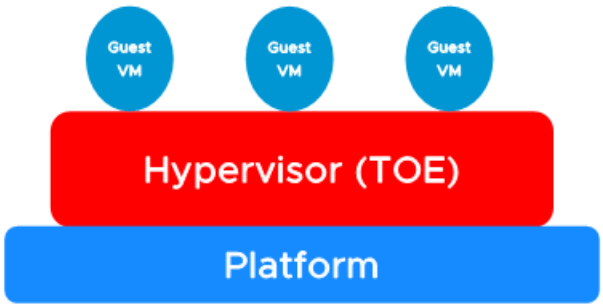

Figure 1: TOE Boundary

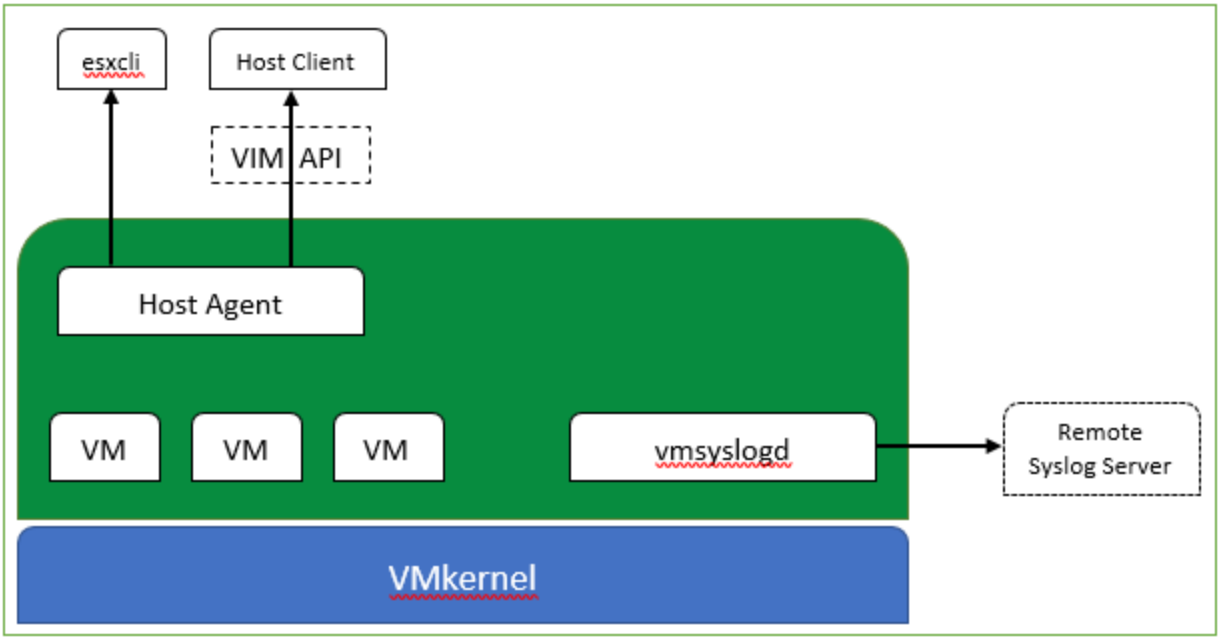

Figure 2: TOE External Interfaces and Internal Components

The physical hardware platform for this evaluation is a Dell PowerEdge R740 server with Intel Xeon Gold 6230R "Cascade Lake" CPUs. This CPU family was selected to provide the Intel VT and EPT feature support required by ESXi, as well as the RDSEED instruction used as an entropy source both internally and as a passthrough entropy source for virtual machines.

4 Security Policy

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

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Security Audit

The TOE's security audit function accepts audit records and stores them locally in pre-allocated files, as well as transmitting them to a remote syslog server via TLS. Each audit record contains relevant information about the audit event. Locally-stored audit records are reviewable by authorized subjects and protected from unauthorized deletion and modification.

4.2 Cryptographic Support

The TOE implements CAVP-validated cryptographic algorithms for its cryptographic services. These are used to support TLS and HTTPS communications. Trusted communications protocols are implemented using secure cryptographic parameters and in accordance with relevant standards. The TOE implements a NIST SP 800-90A conformant DRBG that is seeded with a combination of hardware and software entropy. The hardware entropy source used by the TOE is made available to Guest VMs through a passthrough interface.

4.3 User Data Protection

The TOE uses hardware-based mechanisms to constrain direct access of Guest VMs to PCI devices. Authorized subjects may configure a specific Guest VM to use USB and network interfaces, however access to PCI pass-through devices, vGPU devices, and SCSI pass-through devices is always prohibited. The TOE clears all volatile and non-volatile memory cleared prior to allocation to a Guest VM so that domain separation between Guest VMs is enforced.

4.4 Identification and Authentication

To control access to the TSF, the TOE uses locally defined username/password credentials for authentication. All TSF-mediated actions require successful authentication prior to authorization. The TSF protects against brute-force password authentication attempts by locking an offending user account for a period of time when an excessive number of failed attempts have been accumulated. The TSF also enforces configuration of password complexity policies to further reduce the chance that a brute force authentication attack will succeed.

The TOE uses X.509 certificate validation services for TLS authentication and code signing. CRLs are used for revocation checking. The TSF rejects invalid certificates and those whose revocation status cannot be determined.

4.5 Security Management

The TOE includes management functions that allow for configuration of its own behavior as well as configuration and manipulation of Guest VMs, such as starting/stopping VMs, creating checkpoints for VMs, and configuring the VMs with virtual networking and physical device access. The TOE includes several management interfaces over which various management functions can be performed. The TOE implements role-based access control to grant members of different roles granular privileges to manage the TSF and its associated data. For the purpose of the evaluation, only the ‘Administrator’ role is defined.

The TOE also enforces physical and logical separation of management and operational networks and protects against data sharing between Guest VMs using virtual networking, unless specifically authorized by an Administrator.

4.6 Protection of the TSF

The TOE implements various mechanisms to protect itself from misuse. A Guest VM can only access devices assigned to it by an Administrator. Furthermore, the TOE validates parameters passed to virtual devices, and implements controls for transferring removable media between Guest VMs. The TOE includes an administratively configurable hypercall interface that allows Guest VMs to interact with the hypervisor. The TOE also uses hardware assists to eliminate the need for shadow page tables and reduce the use of binary translation.

The TOE enforces isolation between Guest VMs and between VMs and itself. It also implements various protection methods in the execution environment to protect against memory-based attacks. TOE updates are also integrity protected using code signing certificates.

4.7 TOE Access

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

4.8 Trusted Path/Channels

The TOE implements TLS and HTTPS for secure communications between itself and external entities, which include remote administrators and remote audit servers. The TOE also enforces unambiguous identification of Guest VMs to reduce the likelihood that a user will inadvertently input data to an unintended Guest VM.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The platform has not been compromised prior to installation of the VS.
- Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance.
- 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.

5.2 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:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified in the following documents:
  - *Protection Profile for Virtualization*, Version 1.1, 14 June 2021 ([5])
  - *Supporting Document Mandatory Technical Document PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021 ([7])
  - *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([8])
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in VMware ESX1 7.0 Update 3d Security Target, Version 1.0, 22 July 2022 ([9]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- 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.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.
- The TOE was evaluated on Intel Xeon 6230R “Cascade Lake” CPU. Usage of other Intel CPUs is subject to equivalence arguments which are outside the scope of this evaluation.
- Usage of AMD CPUs is outside the scope of this evaluation. Though VMware ESXi supports AMD CPUs with AMD-V, this configuration is not evaluated and thus usage of AMD CPUs is not NIAP-certified.

6 Documentation

The vendor provides guidance documents describing the installation process for VMware ESXi 7.0 Update 3d, as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation is as follows:

- Guidance Supplement for VMware ESXi 7.0 Update 3d, Version 1.0, 25 July 2022 ([10]).

To use the product in the evaluated configuration, configure it as specified in this document. This document serves as a supplement to the standard VMware documentation set and as such references (either implicitly or explicitly) the following documents:

- VMware ESXi Installation and Setup, Update 3, August 27, 2020
- VMware ESXi Upgrade, Update 3, August 27, 2020
- vSphere Security, Update 3, Jul 12, 2022
- vSphere Single Host Management – VMware Host Client, 28 October 2021
- vSphere Virtual Machine Administration, August 28, 2020.

Note that VMware provides both HTML and PDF versions of these documents. 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 at https://docs.vmware.com/en/VMware-vSphere/index.html.

Any additional documentation provided with the product, or that may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

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

- *VMware ESXi 7.0 Update 3d Common Criteria Test Report and Procedures for Protection Profile for Virtualization, Version 1.1, with PP-Module for Server Virtualization, Version 1.1*, Version 1.0, 26 July 2022 ([13]).

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for VMware ESXi 7.0 Update 3d*, Version 1.0, 28 July 2022 ([12]).

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to:

- *PP-Configuration for Virtualization and Server Virtualization Systems*, Version 1.0, 4 June 2021, which contains the following:
  - *Protection Profile for Virtualization*, Version 1.1, 14 June 2021 ([5])
  - *PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021 ([6])
  - *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([8])

The evaluation team devised a Test Plan based on the Test Activities specified in the above PP and Functional Package, along with *Supporting Document Mandatory Technical Document: PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021 ([7]). The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from May 2021 through August 2022.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising the TOE running on a Dell PowerEdge R740 server platform with an Intel Xeon 6230R (Cascade Lake microarchitecture) CPU. The Assurance Activities Report ([12]) provides a detailed description of the test configuration the CCTL used to test the TOE.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE comprises VMware ESXi 7.0 Update 3d, installed on a Dell PowerEdge R740 server platform with Intel Xeon 6230R "Cascade Lake" CPUs.

The TOE specifies only the above Intel Xeon 6230R "Cascade Lake" CPU. Usage of other Intel CPUs is subject to equivalence arguments that are outside the scope of this evaluation. Usage of AMD CPUs is outside the scope of this evaluation. Although VMware ESXi supports AMD CPUs with AMD-V, this configuration is not evaluated and thus usage of AMD CPUs is not NIAP-certified.

8.2 Excluded Functionality

VMware ESXi additionally includes the following features that are not part of the evaluated TOE because they are outside the scope of the functionality described by the TOE's conformance claims:

- 3rd Party Virtual Infrastructure Bundles (VIBs) (distributed independently of VMware ESXi)
- Active Directory integration
- Common Information Model (CIM)
- Direct Console User Interface
- IPsec
- NSX software
- PCI passthrough (i.e., VMDirectPath I/O), including vGPU
- Physical optical drives (CD/DVD)
- Raw disks (RDM passthrough of storage LUNs)
- Remote shell (SSH)
- SCSI passthrough
- Simple Network Management Protocol (SNMP)
- USB passthrough
- vCenter Server software
- Virtual Shared Disks (Multiwriter disks)
- VM encryption
- VM Virtual Disk sharing
- vMotion
- VMware PowerCLI software
- vSAN software.

Additionally, the Guest VM software is not provided by VMware. Customers supply their own operating systems from 3rd party operating system vendors (e.g., Microsoft Windows Server 2016 or Red Hat Enterprise Linux 8). Guest VMs and their contents are outside the scope of the TOE.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for VMware ESXi 7.0 Update 3d ([11]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in the following documents:

- *Protection Profile for Virtualization*, Version 1.1, 14 June 2021 ([5])
- *Supporting Document Mandatory Technical Document PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021 ([7])
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 ([8]).

The evaluation determined the TOE satisfies the conformance claims made in the VMware ESXi 7.0 Update 3d Security Target, of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in *PP-Configuration for Virtualization and Server Virtualization Systems*, Version 1.0, 4 June 2021, which contains the following:

- *Protection Profile for Virtualization*, Version 1.1, 14 June 2021
- *PP-Module for Server Virtualization Systems*, Version 1.1, 14 June 2021
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PPs, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV evaluation activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance evaluation activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC evaluation activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit to the extent possible given the evaluation evidence required by the claimed PP. Additionally, the evaluation team performed the ALC_TSU_EXT.1 evaluation activity specified in [5]. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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

The evaluation team performed each test activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of public vulnerability databases.

The evaluation team conducted a search of the National Vulnerability Database (http://web.nvd.nist.gov/view/vuln/search) on 28 July 2022, using the following search terms:

- vmware esxi 7.0.0
- vmware esxi 7.0
- esxi 7.0
- vmdk
- virtual machine disk
- virtual machine manager
- vcenter server
- dell poweredge r740 server
- intel xeon gold 6230.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed PP. Furthermore, the evaluation team's testing demonstrates 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 validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Security Target

The ST for this product's evaluation is *VMware ESXi v7.0 Update 3d Security Target*, Version 1.0, 22 July 2022 ([9]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PCI	Peripheral Component Interconnect
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VIB	Virtual Infrastructure Bundle
VM	Virtual Machine
VR	Validation Report
VS	Virtualization System

13 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

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

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

[5] Protection Profile for Virtualization, Version 1.1, 14 June 2021.

[6] PP-Module for Server Virtualization Systems, Version 1.1, 14 June 2021.

[7] Supporting Document Mandatory Technical Document PP-Module for Server Virtualization Systems, Version 1.1, 14 June 2021

[8] Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019.

[9] VMware ESXi v7.0 Update 3d Security Target, Version 1.0, 22 July 2022.

[10] Guidance Supplement for VMware ESXi v7.0 Update 3d, Version 1.0, 25 July 2022.

[11] Evaluation Technical Report for VMware ESXi v7.0 Update 3d, Version 1.0, 28 July 2022.

[12] Assurance Activities Report for VMware ESXi v7.0 Update 3d, Version 1.0, 28 July 2022.

[13] *VMware ESXi 7.0 Update 3d Common Criteria Test Report and Procedures for Protection Profile for Virtualization, Version 1.1, with PP-Module for Server Virtualization, Version 1.1*, Version 1.0, 26 July 2022.