National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

VMware Horizon Client 8 2209 (Horizon 8.7)

Report Number:	CCEVS-VR-VID11357-2023
Dated:	June 16, 2023
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

Jenn Dotson

Sheldon Durrant

Lisa Mitchell

Linda Morrison

Clare Parran

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.

Columbia, MD

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of VMware Horizon Client 8 2209 (Horizon 8.7) (the Target of Evaluation (TOE)) evaluation. 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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in June 2023. 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 following documents:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021
- *Functional Package for Transport Layer Security (TLS),* Version 1.1, February 12, 2019

The TOE is VMware Horizon Client 8 2209 (Horizon 8.7). 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). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme 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 Security Target (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 technical information included in this report was obtained from the *VMware Horizon Client 8 2209 (Horizon 8.7) Security Target*, Version 1.0, 04 April 2023, and analysis performed by the Validation team.

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) using the Common Evaluation Methodology (CEM) 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 Validated Products List.

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 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 Horizon Client 8 2209 (Horizon 8.7)
Security Target	*VMware Horizon Client 8 2209 (Horizon 8.7) Security Target*, Version 1.0, 4 April 2023
Evaluation Technical Report	*Evaluation Technical Report for VMware Horizon Client 8 2209 (Horizon 8.7)*, Version 1.0, 13 June 2023
Sponsor & Developer	VMware, Inc. 3401 Hillview Avenue Palo Alto, CA 94304
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
Protection Profile	*Protection Profile for Application Software*, Version 1.4, 7 October 2021 *Functional Package for Transport Layer Security (TLS),* Version 1.1, February 12, 2019
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046

Item	Identifier
Evaluation Personnel	Dawn Campbell, Kevin Zhang, Pascal Patin
Validation Personnel	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Linda Morrison, Clare Parran, Chris Thorpe

3 TOE Architecture

The Horizon Client TOE consists of the Horizon Client application, specifically version 2209 or 8.7. The TOE has both Windows and Android platform versions. Both platform versions consist of C and C++ code; the Android platform version also has Java components and the Windows platform version also has C++/CLI and C# components. All third-party components used by the TOE (as specified by Appendix A.2 in the Security Target) are linked into the TOE binaries; the sole executable process is the TOE itself.

3.1 Physical Boundary

The VMware Horizon Client 8 application resides on the end user device and is used to access enterprise resources. A user accesses their virtual desktop through the Horizon Client. The virtual desktop consolidates the users authorized enterprise computing environments and applications into a single view that is presented to them through the client application. In the evaluated configuration, users interact with resources on their virtual desktop using the VMware Blast Extreme protocol (“Blast protocol”), which is a VMware proprietary encoding protocol for real-time streaming of video data from a remote device.

The VMware Horizon Client 8 application is part of the VMware Horizon suite of applications consisting of Horizon Client applications, Horizon Agent applications, and Horizon Connection Server(s). A VMware Horizon deployment typically includes one or more instances of the VMware Unified Access Gateway (UAG) as well. Figure 1 shows the TOE in a sample deployment with other VMware Horizon applications and the UAG in its operational environment.

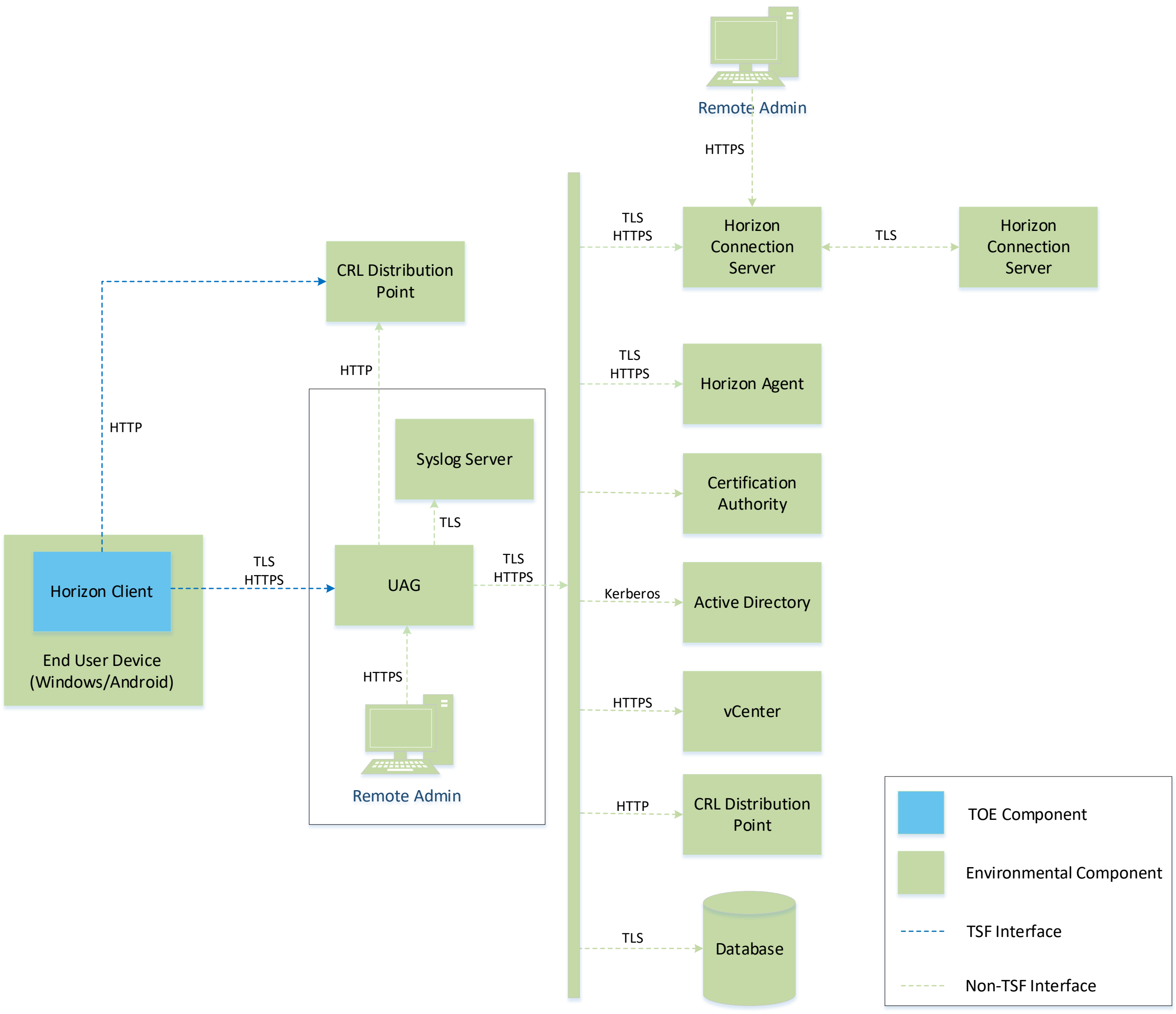


Figure 1: TOE Boundary

The TOE has the following system requirements for its host platform:

- x86-based processor with 800MHz or higher clock speed (Windows), x86-based or ARM-based processor (Android) – note that the tested Windows platform used 64-bit x86 and the tested Android platform used arm64
- 1 GB RAM
- Windows 10 or Android 11, depending on platform version
- Platform must be configured into FIPS-compliant mode of operation (Windows)
- .NET Framework version 4.5 or later (Windows)
- H.264 codec support

The following network ports must be open for the TOE to function:

- TCP/443 (for initial connection to Connection Server via UAG and Blast protocol connectivity to Horizon Agent via UAG)

The TOE's operational environment includes the following:

- Other VMware Horizon components (at least one each of Horizon Connection Server and Horizon Agent).
- Network access to other VMware Horizon components mediated through at least one VMware UAG.
- Platform (hardware and software) on which the TOE is hosted.
    - The TOE is capable of running on a general-purpose Windows or Android operating system on standard consumer-grade hardware. For the evaluated configuration, the TOE was tested on the following environments:
        - Windows 10: Intel Core i7-10850H (10th Gen, Comet Lake) processor on Dell Precision 5550
        - Android 11: Samsung Exynos 9820 (M4, Cortex-A75, Cortex-A55) processor on Samsung Galaxy S10 5G Module/SKU SM-G977N
- Access to a Certification Authority and corresponding revocation checking mechanism is needed to validate presented X.509 certificates.

4 Security Policy

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

4.1 Cryptographic Support

The TOE implements cryptography to protect data in transit. For data in transit, the TOE implements TLS/HTTPS as a client. The TOE supports mutual authentication for its TLS connections.

The TOE implements all cryptography used for these functions using its own implementations of OpenSSL with NIST-approved algorithms. The TOE's DRBG is seeded using entropy from the underlying OS platform.

For data at rest, the TOE relies on its operational environment to control access to stored credential data.

4.2 User Data Protection

The TOE relies on platform credential storage mechanisms to protect sensitive data at rest.

The TOE relies on the network connectivity of its host OS platform. The TOE can also access the system clipboard (depending on administrative configuration), audio/video capture devices, and attached USB storage devices and file system resources.

4.3 Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS/HTTPS connections. The TOE relies on platform-provided functionality to support various certificate validity checking methods, including the checking of certificate revocation status using CRL. If the validity status of a certificate cannot be determined, the certificate will be accepted or rejected based on administrative configuration. All other cases where a certificate is found to be invalid will result in rejection without an administrative override.

4.4 Security Management

The TOE itself and the configuration settings it uses are stored in locations recommended by the platform vendor. The TOE is launched by an authenticated OS user and runs in the session context of that user; there is no interface for a non-administrator to act as an administrator through separate authentication. When in its evaluated configuration, the TOE does not have any security-relevant management functions as all security-relevant configuration is done as part of the initial setup of the TOE.

4.5 Privacy

The TOE does not have an interface to request or transmit requested PII from a user; PII is only transmitted over the network if initiated by the user.

4.6 Protection of the TSF

The TOE enforces various mechanisms to prevent itself from being used as an attack vector to its host OS platform. The TOE implements address space layout randomization (ASLR), does not allocate any memory with both write and execute permissions, does not write user-modifiable files to directories that contain executable files, is compiled using stack overflow protection, and is compatible with the security features of its host OS platform.

The TOE contains libraries and invokes system APIs that are well-known and explicitly identified.

The TOE has a mechanism to determine its current software version. Software updates to the TOE can be acquired through the application itself or by leveraging its OS platform, depending on the platform version of the TOE. All updates are digitally signed to guarantee their authenticity and integrity.

4.7 Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS/HTTPS. These interfaces are used to secure all data in transit between the TOE and its operational environment.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *Protection Profile for Application Software*, Version 1.4, 07 October 2021

That information has not been reproduced here and PP_APP_V1.4 should be consulted if there is interest in that material.

As a functional package, the TLS Package does not contain a Security Problem Definition. The TOE's use of TLS is intended to mitigate the T.NETWORK_ATTACK and T.NETWORK_EAVESDROP threats defined by PP_APP_V1.4.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP_APP_V1.4/FP_TLS_V1.1 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 (the assurance activities specified in the PP_APP_V1.4/FP_TLS_V1.1 and performed by the Evaluation team).
- This evaluation only covers the software version and platform versions identified in this document and referenced in the *VMware Horizon Client 8 2209 (Horizon 8.7) Security Target*, Version 1.0, 4 April 2023, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific software version and platform versions was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the PP_APP_V1.4/FP_TLS_V1.1 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *VMware Horizon Client 8 2209 (Horizon 8.7) Common Criteria (CC) Evaluated Configuration Guide* Version 1.0, April 4, 2023
- *VMware Horizon 2209 Installation and Upgrade,* 2022
- *VMware Horizon Client for Windows 2209, Horizon Client for Windows User Guide,* 2022
- *VMware Horizon Client for Android 2209, Horizon Client for Android User Guide*, 2022
- VMware *Horizon 2209 Horizon Security*, 2022
- *VMware Horizon 2209 Horizon Overview and Deployment Planning*, 2022
- *VMware Horizon 2209 Horizon Administration*, 2022

To use the product in the evaluated configuration, the product must be installed and configured as specified in *VMware Horizon Client 8 2209 (Horizon 8.7) Common Criteria (CC) Evaluated Configuration Guidance*. This document provides references to other documentation for specific steps in to place the TOE into its the evaluated configuration and these documents are provided on 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 Horizon Client 8 Common Criteria Test Report and Procedures*, Version 1.0, April 21, 2023

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

- *Assurance Activities Report for VMware Horizon Client 8 2209 (Horizon 8.7)*, Version 1.0, 13 June 2023

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

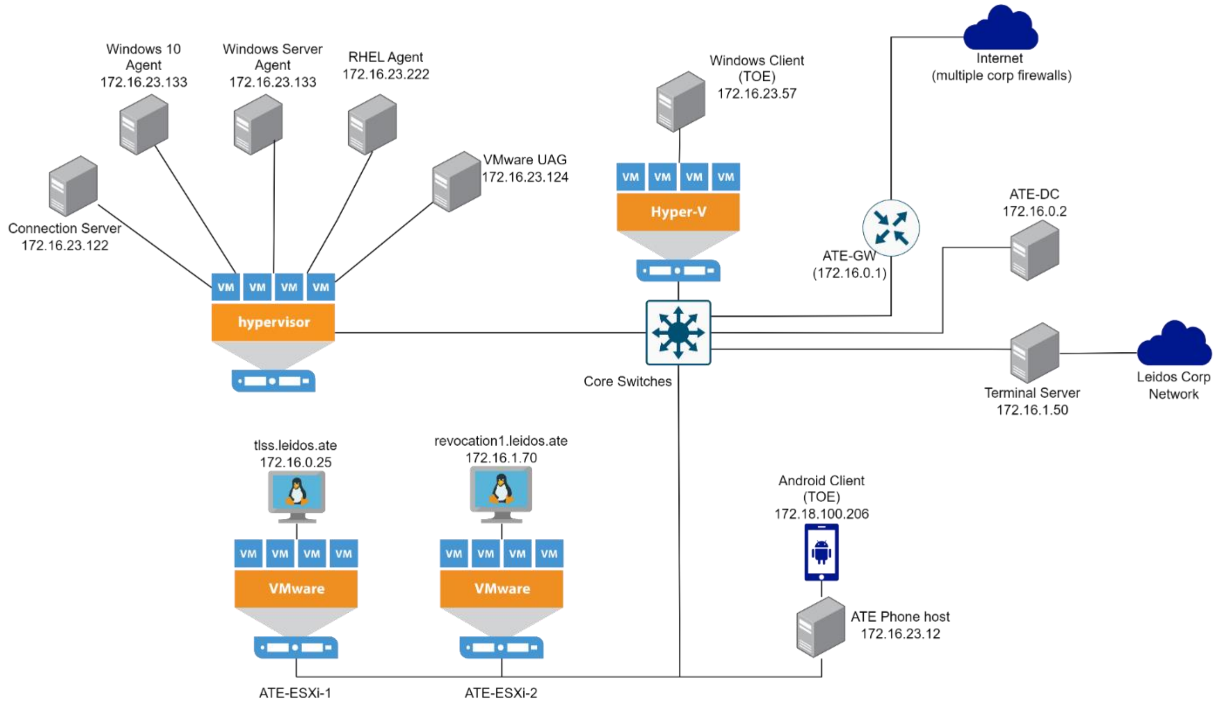
The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the PP_APP_V1.4/FP_TLS_V1.1.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from May 20, 2022 to April 11, 2023.

The Evaluation team 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.

7.3 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration.



The following components were used to create the test configurations:

TOE Devices

VMware Windows Client
Purpose: TOE
IP / MAC: 172.16.23.57 / 8C:AE:4C:E1:70:84
Version: 2209.1

VMware Android Client
Purpose: TOE
IP / MAC: 172.18.100.206 / BE:C6:70:E3:22:8B
Phone model: Galaxy S10 5G
OS: Android 11

Environment Devices

- VMware Hypervisor

  Purpose: TOE host

  IP / MAC: 172.16.23.232 / 78:AC:44:41:B7:68

  ESXi Version: 7.0
- Hyper-V

  Purpose: Hosting server

  IP / MAC: 172.16.50.10 / DC:F4:01:E8:60

Version: Windows Server Datacenter 10.0.18363

- ATE Phone Host server
  Purpose: Virtualization server
  IP / MAC: 172.16.23.12 / 8C:AE:4C:E1:70:84
  Version: Windows 10 Professional
- Windows 10 Agent
  Purpose: Connection target for TOE
  IP / MAC: 172.16.23.131 / 00:50:56:88:69:92
  Version: 2209.1
  ESXi Version: 7.0.2
- Windows Server Agent
  Purpose: Connection target for TOE
  IP / MAC: 172.16.23.133 / 00:0C:29:52:6B:B4
  Version: 2209.1
  ESXi Version: 7.0.2
- RHEL Agent
  Purpose: Connection target for TOE
  IP / MAC: 172.16.23.222 / 00:0C:29:A):F4:04
  Version: 2209.1
  ESXi Version: 7.0.2
- VMware Connection Server
  Purpose: Virtualization server
  IP / MAC: 172.16.23.12 / 00:50:56:88:36:BC
  Version: 2209.1
- VMware Unified Access Gateway (UAG)
  Purpose: Virtualization server
  IP / MAC: 172.16.23.124 / 00:50:56:A7:F1:85
  Version: 2209.2
- ATE-GW (Physical)
  Purpose: Main router/gateway
  IP/ MAC: 172.16.0.1 / ac:1f:6b:95:0c:1d
  OS: PfSense 2.4.4-RELEASE-p2
- ATE-DC (Physical)
  Purpose: Main Domain Controller (DC) for Test environment/DNS server
  IP /MAC: 172.16.0.2 / 00:22:19:58:EB:8D
  OS: Windows Server 2016 version 1607
  Protocols used: RDP, DNS

- ATE-ESXi-1 (Physical)
  Purpose: Virtualization server
  IP/ MAC: 172.16.1.62 / 10:7b:44:92:77:bf
  OS: VMware ESXi, 6.5.0, 5969303
- Terminal Server (Physical)
  Purpose: Provide tester access to the Test Environment from corporate network.
  IP/MAC: 172.16.1.50 / D4:BE:D9:B4:FE:66
  OS: Windows server 2016 version 1607
  Protocols used: RDP
- TLSS.leidos.ate (VM)
  Purpose: Hosts TLS Test Tools
  IP/MAC: 172.16.0.25 / 00:50:56:b1:66:0b
  OS: Ubuntu 18.04.5
  Protocols Used: TLS
  Relevant Software:
  Proprietary Python TLS test tools
  OpenSSL 1.1.1
  Wireshark 2.6.10

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is the VMware Horizon Client 8 2209 (Horizon 8.7), evaluated on the following host platforms:

- Windows platform:
    - Windows 10
    - Platform configured into FIPS-compliant mode of operation
    - Intel Core i7-10850H (10th Gen, Comet Lake) processor
- Android platform:
    - Android 11
    - Samsung Exynos 9820 (M4, Cortex-A75, Cortex-A55) processor

8.2 Excluded Functionality

The TOE has the following logical exclusions:

- Tunnel Channel – The Horizon Client has a separate tunnel channel that allows for communications of Microsoft RDP and Windows Media MMR through HTTPS. This channel also allows a USB device connected to the end user workstation to be accessible on the virtual desktop as if it was plugged in to the remote device (USB redirection), and it allows for the Horizon Client's local file system to be similarly accessible on the virtual desktop (Client Drive Redirection, or CDR). In the evaluated configuration, the communications that use the tunnel channel are configured to use Blast instead.
- PCoIP – The Horizon Client supports PC over IP (PCoIP) for remote communications with Horizon Agents. In the evaluated configuration, this is disabled on the server side of the connection and Blast is used instead.
- Direct Connection Server Interface – Depending on network architecture, a Horizon Client may be configured to communicate directly with a Connection Server as part of establishing a connection to a Horizon Agent. In the evaluated configuration, this particular deployment is not used and all communications from the Horizon Client are routed through a UAG.

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 Horizon Client 8 2209 (Horizon 8.7)*. 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 and CEM version 3.1, revision 5, and the specific evaluation activities specified in the PP_APP_V1.4/FP_TLS_V1.1.

The evaluation determined the TOE satisfies the conformance claims made in the VMware Horizon Client 8 2209 (Horizon 8.7) Security Target, of Part 2 extended and Part 3 extended. The Validation Team 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 assurance 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 Protection Profile, and security function descriptions that satisfy the requirements.

The Validation team 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 performed each ADV assurance 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 Protection Profile 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.

The Validation team 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 performed each guidance assurance 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.

The Validation team 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 performed each ALC assurance 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 Protection Profile. 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.

The Validation team 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 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 PP-Module and recorded the results in the Test Report, summarized in the AAR.

The Validation team 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 (AVA)

The evaluation team performed each AVA evaluation 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 performed a search of the following public vulnerability databases:

- National Vulnerability Database (https://nvd.nist.gov/),
- OpenSSL.org (https://www.openssl.org/news/vulnerabilities.html), and
- VMware’s Security Advisories page: https://www.vmware.com/security/advisories.html.

Searches were performed on 20 April 2023 and 7 June 2023, using the following search terms:

- VMware Horizon
- Horizon Client
- VMware's OpenSSL FIPS Object Module 2.0.20-vmw
- Centralized content server
- Enterprise resource delivery
- Enterprise content delivery
- OpenSSL 1.0.2zg (third party library)
- Third Party Libraries identified in Section A.2 of the Security Target

The Evaluation team determined that that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

The Validation team 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, sufficient to satisfy the assurance activities specified in the claimed Protection Profile and PP-Module. 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 Validation team suggests 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 security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in *VMware Horizon Client 8 2209 (Horizon 8.7) Common Criteria (CC) Evaluated Configuration Guide Version 1.0, April 4, 2023*. As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later were evaluated.

Any additional customer documentation, not listed in Section 6, provided with the product, or that which 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.

11 Security Target

The ST for this product's evaluation is *VMware Horizon Client 8 2209 (Horizon 8.7) Security Target*, Version 1.0, 4 April 2023.

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

13 Bibliography

[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 Application Software*, Version 1.4, 07 October 2021.

[6] *VMware Horizon Client 8 2209 (Horizon 8.7) Security Target*, Version 1.0, 4 April 2023.

[7] *VMware Horizon 2209 Installation and Upgrade*, 2022.

[8] *VMware Horizon 2209 Horizon Security*, 2022

[9] *VMware Horizon Client 8 2209 (Horizon 8.7) Common Criteria (CC) Evaluated Configuration Guidance,* Version 1.0, April 4, 2023.

[10] *Evaluation Technical Report for VMware Horizon Client 8 2209 (Horizon 8.7)*, Version 1.0, 13 June 2023.

[11] *Assurance Activities Report for VMware Horizon Client 8 2209 (Horizon 8.7), Version 1.0*, 13 June 2023.

[12] *VMware Horizon Client 8 Common Criteria Test Report and Procedures*, Version 1.0, 21 April 2023.

[13] *VMware Horizon Client for Windows 2209, Horizon Client for Windows User Guide*, 2022

[14] *VMware Horizon Client for Android 2209, Horizon Client for Android User Guide*, 2022

[15] *VMware Horizon 2209 Horizon Overview and Deployment Planning*, 2022

[16] *Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019*

[17] *VMware Horizon 2209 Horizon Administration*, 2022

[18] *VMware Horizon Client Vulnerability Analysis*, Version 1.1, June 13, 2023