National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

VMware Unified Access Gateway (UAG) 2209

Report Number: CCEVS-VR-VID11360-2023
Dated: July 6, 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 George, 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 Unified Access Gateway (UAG) 2209 (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.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in July 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 Conformant and meets the assurance requirements of the following documents:

- *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020* (CPP_ND_V2.2e)

The TOE is VMware Unified Access Gateway (UAG) 2209. 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 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 Unified Access Gateway (UAG) Security Target*, Version 1.0, 24 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, 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 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).

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 Unified Access Gateway (UAG) 2209
Security Target	VMware Unified Access Gateway (UAG) 2209 Security Target, Version 1.0, 24 April 2023
Evaluation Technical Report	Evaluation Technical Report for VMware Unified Access Gateway (UAG) 2209, Version 1.0, 23 June 2023
Sponsor & Developer	VMware, Inc. 3401 Hillview Avenue Palo Alto, CA 94304
Completion Date	July 6, 2023
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	*collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020
Conformance Result	PP Compliant, CC Part 2 Extended, CC Part 3 Conformant

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
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 UAG TOE a virtual network device running on an environmental hypervisor and physical platform. The TOE software includes VMware Photon 3.0, OpenSSL and Bouncy Castle BC-FJA cryptographic libraries, as well as specialized software needed to run the actual UAG functionality.

3.1 Physical Boundary

The TOE is the VMware UAG 2209. Specifically, the TOE is a virtual network device that includes its operating system (VMware Photon 3.0) and the software that runs on it. The TOE boundary therefore includes only the virtualized network device, while its underlying hypervisor and physical platform are environmental. It is part of the VMware Horizon suite of applications consisting of Horizon Client applications, Horizon Agent applications, and Horizon Connection Server(s).

Figure 1 shows the TOE in a sample deployment with other VMware Horizon components in its operational environment.

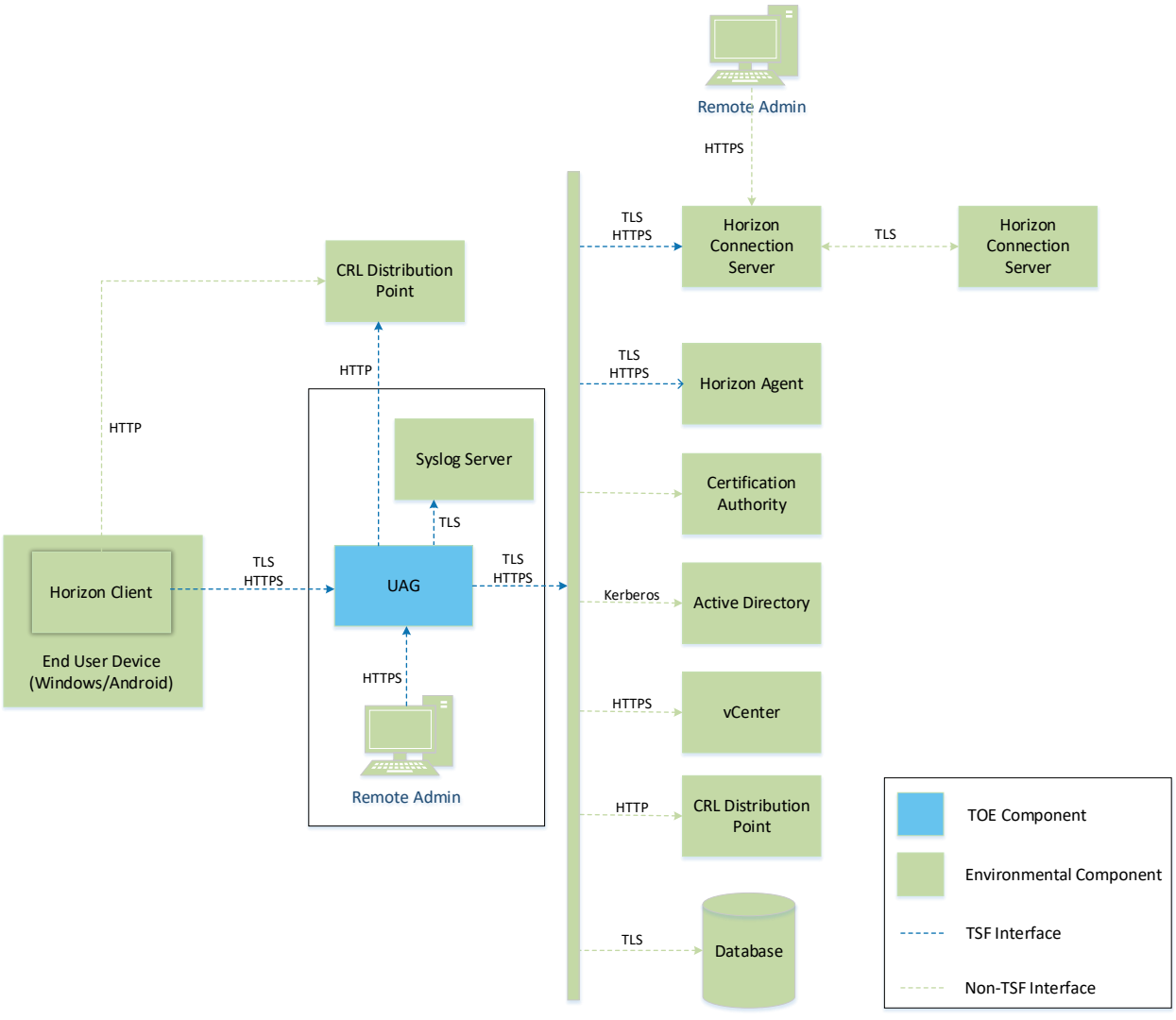

Figure 1: TOE Boundary

The TOE handles inbound requests from the Horizon Client over both mutually-authenticated and one-way TLS. Initial Horizon Client connectivity to the TOE requires mutually-authenticated TLS but once authenticated, subsequent connections do not require re-validation of the client certificate. Inbound management communications and outbound communications, both to the environmental syslog server and to other Horizon components (Connection Server and Agent) use one-way TLS. While the TOE does not provide a certificate to a remote Horizon Agent for authentication, the Horizon Agent does require it to provide a single use authorization token that is issued to the TOE by the Connection Server.

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

- TCP/443 (for inbound session establishment connectivity and Blast protocol connectivity from Horizon Clients)
- TCP/9443 (for inbound remote administration)

The TOE's operational environment includes the following:

- VMware Horizon components (at least one each of Horizon Client, Horizon Connection Server, and Horizon Agent)
- Remote syslog server
- Platform (hardware and software) on which the TOE is hosted. In the tested configuration, this included the following:
    - VMware ESXi 7.0
    - Dell PowerEdge R740 with Intel Xeon 6230R (Cascade Lake) processor
- Access to a Certification Authority and corresponding revocation checking mechanism is needed to validate presented X.509 certificates.
- A remote system with a supported web browser for remote administrative access:
    - The tested configuration used Google Chrome 106.0.5249.119

4 Security Policy

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

4.1 Security Audit

The TOE generates audit records of security-relevant activity. Audit data is stored locally on the TOE in several different files based on event type; local audit records are protected against unauthorized modification and deletion. A log rotation exists to overwrite the oldest stored records when audit storage space has been exhausted. The TOE also has the ability to export all audit records to an external syslog server over a TLS protected channel.

4.2 Cryptographic Support

The TOE implements cryptographic functions in support of trusted communications, key pair generation for X.509 certificate requests, and self-testing. The TOE includes both OpenSSL and Bouncy Castle BC-FJA cryptographic libraries. For trusted communications, the TOE implements TLS as a server with HTTPS, and TLS as a client with and without HTTPS. TLS/HTTPS server connectivity between the environmental Horizon Client and the TOE enforces mutual authentication of TLS client certificates. The TOE relies on platform hardware to generate entropy that is used to seed its DRBG to ensure that generated keys have the advertised security strength.

4.3 Identification and Authentication

The TOE uses a local password-based mechanism for administrator authentication. The TOE enforces restrictions on the length and character composition of administrator passwords. Excessive failed authentication attempts on a remote administrative interface will cause a lockout that is resolved by a waiting period. The TOE also uses X.509 certificates for authentication of TLS connections. The TOE has a mechanism by which a certificate signing request can be generated so that it may obtain a certificate for its own use from a trusted CA.

4.4 Security Management

The TOE has a web-based remote management interface as well as a local console. Most functionality is administered over the remote interface. The TOE uses a single Security Administrator role to authorize the use of management functions.

4.5 Protection of the TSF

The TOE protects sensitive data from unauthorized access. It enforces integrity of its own contents through the use of self-tests to ensure that the TSF has not been modified. Software updates are obtained through the operational environment (e.g. downloaded from the vendor's support site); updates have a published hash that an administrator can verify prior to their application.

4.6 TOE Access

The TOE controls access through enforcement of idle session timeout on its management interfaces. These interfaces also display a configurable pre-authentication warning banner that advises against unauthorized use of the TOE.

4.7 Trusted Path/Channels

The TOE implements TLS and TLS/HTTPS trusted channels between itself and environmental systems. The TOE also implements a TLS/HTTPS trusted path for secure remote administration.

5 Assumptions and Clarification of Scope

5.1 Assumptions

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

- *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020*

That information has not been reproduced here and CPP_ND_V2.2e should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the CPP_ND_V2.2e 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 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 (the assurance activities specified in the CPP_ND_V2.2e and performed by the Evaluation team).
- This evaluation covers only the specific software distribution and version identified in this document and referenced in the *VMWare Unified Access Gateway (UAG) 2209 Security Target*, Version 1.0, April 24, 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 CPP_ND_V2.2e 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 Unified Access Gateway (UAG) 2209 Common Criteria (CC) Evaluated Configuration Guidance, Version 1.0, April 24, 2023*
- *Deploying and Configuring VMware Unified Access Gateway, 2023*
- *Horizon Administration VMware Horizon 2209, 2022*

To use the product in the evaluated configuration, the product must be installed and configured as specified in *VMware Unified Access Gateway (UAG) 2209 Common Criteria (CC) Evaluated Configuration Guide*. This document provides references to other documentation for specific steps to place the TOE into its the evaluated configuration.

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 8 UAG Common Criteria Test Report and Procedures, Version 1.0, 5 July 2023.*

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

- *Assurance Activities Report for VMware Unified Access Gateway (UAG) 2209*, Version 1.0, 23 June 2023

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 the following specifications:

- *collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020

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 CPP_ND_V2.2e.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from May 2, 2022 to July 5, 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.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is the VMware UAG 2209. The specific tested version is “Unified Access Gateway (UAG) 2209.2 for vSphere (FIPS)”. The TOE is a virtualized network device evaluated on the following host platform:

- VMware ESXi 7.0
- Dell PowerEdge R740 with Intel Xeon 6230R (Cascade Lake) processor

8.2 Excluded Functionality

The product has a variety of uses but the purpose of the TOE as evaluated is for facilitating connectivity between VMware Horizon users and virtual desktops/applications.

The TOE conforms to the CPP_ND_V2.2e. As such, the security-relevant functionality of the product is limited to the claimed requirements in this standard. All functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target.

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 Unified Access Gateway (UAG) 2209, Version 1.0, 23 June 2023. 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 CPP_ND_V2.2e.

The evaluation determined the TOE satisfies the conformance claims made in the VMware Unified Access Gateway (UAG) 2209 Security Target, of Part 2 extended and Part 3 Conformant. 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 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 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 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 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 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.

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 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 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 Protection Profile 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 Protection Profile. This comprised a search of public vulnerability databases.

The evaluation team performed a search of the following online sources:

- National Vulnerability Database (https://nvd.nist.gov/), and
- VMware's Security Advisories page: https://www.vmware.com/security/advisories.html.

Searches were performed on 9 May 2023 and again on 22 June 2023, using the following search terms:

- VMware Unified Access Gateway
- VMware UAG
- Unified Access Gateway
- VMware Photon 3.0
- Vmware's OpenSSL FIPS Object Module 2.0.20-vmw
- OpenSSL 1.0.2zg
- BC-FJA
- Intel Xeon 6230R.

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.

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. 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 Security Target, 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 Unified Access Gateway (UAG) 2209 Common Criteria (CC) Evaluated Configuration Guide, Version 1.0, April 24, 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 Unified Access Gateway (UAG) 2209 Security Target*, Version 1.0, 24 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

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] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] VMware Unified Access Gateway (UAG) 2209 Security Target, Version 1.0, 24 April 2023.

[7] Horizon Administration VMware Horizon 2209, 2022.

[8] Evaluation Activities for Network Device cPP, Version 2.2, December 2019.

[9] VMware Unified Access Gateway (UAG) 2209 Common Criteria (CC) Evaluated Configuration Guidance, Version 1.0, April 24, 2023.

[10] Evaluation Technical Report for VMware Unified Access Gateway (UAG) 2209, Version 1.0, 23 June 2023

[11] Assurance Activities Report for VMware Unified Access Gateway (UAG) 2209, Version 1.0, 23 June 2023.

[12] VMware Horizon 8 UAG Common Criteria Test Report and Procedures, Version 1.0, 5 July 2023.

[13] Deploying and Configuring VMware Unified Access Gateway, 2023.