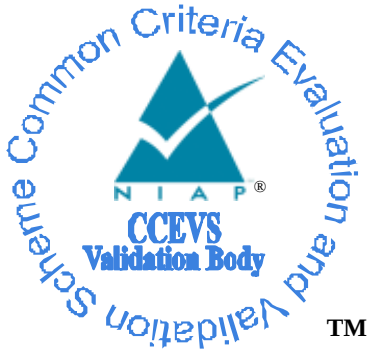
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

for the

Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1

Report Number: CCEVS-VR-11225-2022

Dated: January 26, 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

Jenn Dotson
Sheldon Durrant
Linda Morrison
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Dayanandini Pathmanathan
Rodrigo Tapia
Minal Wankhede
Varsha Shetye
Anthony Busciglio
Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) Validation team assessment of the evaluation of the Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Target of Evaluation (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 completed by the Acumen Security Common Criteria Testing Laboratory (CCTL) Rockville, MD, United States of America, and was completed in January 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the *collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020 [NDcPP22e].

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 (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 that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Security Target,* Version 1.6, 1/24/2022, 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, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile (PP) 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	Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1
Protection Profile	*collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 [NDcPP22e]
Security Target	*Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Security Target*, Version 1.6, 1/24/2022
Evaluation Technical Report	*Evaluation Technical Report for Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1*, Version 1.2, 1/19/2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Citrix Systems Inc.
Developer	Citrix Systems Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Linda Morrison, Clare Parran

3 Architectural Information

The Citrix Application Delivery Controllers (ADC) are purpose-built networking appliances whose function is to improve the performance, security and resiliency of applications delivered over the web. The ADC intelligently distributes, optimizes application performance, enhances application availability with advanced Layer 4 – Layer 7 load balancing, secures applications from attacks, and lowers server expenses by offloading computationally intensive tasks. The TOE comprises Citrix ADC 12.1 software running on the following:

- Physical Platforms
  - MPX 8900 FIPS
  - MPX 15000-50G FIPS
- Virtual Platforms
  - VPX FIPS on ESXi 6.5 running on a Dell PowerEdge R630 Server

Citrix ADC MPX FIPS and Citrix ADC VPX FIPS are network devices and virtual network devices that combine Layer 4 - Layer 7 load balancing and content switching with application acceleration, data compression, static and dynamic content caching, SSL acceleration, network optimization, application performance monitoring, application visibility, and robust application security via an application firewall. The Citrix ADC MPX FIPS & Citrix ADC VPX FIPS appliances support all the NIST-approved FIPS 140-2 algorithms.

3.1 Evaluated Configuration

The TOE evaluated configuration consists of the physical platforms, MPX 8900 FIPS and MPX 15000-50G FIPS. Both, the MPX 8900 FIPS and the MPX 15000-50G FIPS, operate using the Intel® Xeon E5-2620 v4 (Broadwell) processor. Additionally, the evaluated configuration includes the VPX FIPS virtual platform. This virtual platform is hosted within a Dell PowerEdge R630 Server running an instance of VMware ESXi 6.5 hypervisor. The VPX is hosted on a server which operates on an Intel® Xeon E5-2680 v4 (Broadwell) processor. FreeBSD 8.4 is the operating system on all the physical and virtual platforms.

3.2 Excluded Functionality

Hardware and software located in the TOE environment (see Section 1.4 of the ST) are not included in the scope of evaluations.

Only security functionality specified in the SFRs is covered by the scope of evaluation. Any other product features or functionality are considered unevaluated, because they are not included in the scope of the Security Target:

- Web Logging
- Application Firewall
- Global Server Load Balancing (GSLB)
- AAA-TM Authentication
- External authentication methods: Kerberos, TACACS+, SAML, RADIUS
- Responder

- Rewrite (URL Transformation)
- Layer 3 Routing
- Vpath
- RISE
- High Availability
- Cloud Bridge
- CallHome
- Integrated Disk Caching
- General TLS VPN functionality
- Clientless VPN functionality
- SSL acceleration – SSL termination for application servers
- AppFlow
- AppQoE
- BGP
- Cache Redirection
- Compression Control
- Content Accelerator
- Content Filtering
- Content Switching
- FEO
- OSPF
- LSN
- RDP Proxy
- RIP
- HTM Injection
- HTTP DoS Protection
- Integrated Caching
- Surge Protection
- ISIS
- Priority Queuing
- Reputation
- Sure Connect
- NetScaler Push
- ContentInspection
- Connection Quality Analytics
- Adaptive TCP
- Forward Proxy
- Video Optimization
- URL Filtering

Additionally, the following features may not be used when the TOE is operated in a manner compliant with this Security Target:

- IPv6

- NTP based updates to the time
- Use of superuser privileges except as described in [CCECG]
- ADC GUI (HTTP/HTTPS), ADC Nitro API and ADM

4 Security Policy

The TOE provides the security functions required by NDcPP v2.2e, as identified below.

- **Security Audit** - The TOE keeps local and remote audit records of security relevant events. Remote audit records are transferred via TLS to the external audit server.
- **Cryptographic Support** - The TOE provides cryptographic support for the SSH for remote administrative access and TLS connections to external IT devices. The cryptography for the TOE is provided by Citrix ADC CP Cryptographic Library v3.0 and Citrix ADC CP Cryptographic Library v4.0 running on FreeBSD 8.4. This is the underlying OS of the TOE on which the firmware runs.
- **Identification and Authentication** - The TOE provides two types of authentication to provide a trusted means for Security Administrators and remote endpoints to interact:
    - Password-based or public-key authentication for Security Administrators
    - X.509v3 certificate-based authentication for remote devices

  Device-level authentication allows the TOE to establish a secure communication channel with a remote endpoint. Security Administrators can set a minimum length for passwords (between 4 and 127 characters). Additionally, the TOE detects and tracks consecutive unsuccessful remote authentication attempts and will prevent the offending attempts from authenticating when a Security Administrator defined threshold is reached.
- **Security Management** - The TOE enables secure local and remote management of its security functions, including:
    - Local console CLI administration
    - Remote CLI administration via SSHv2
    - Administrator authentication using a local database
    - Timed user lockout after multiple failed authentication attempts
    - Password complexity enforcement
    - Role Based Access Control - the TOE supports several types of administrative user roles. Collectively these sub-roles comprise the “Security Administrator”
    - Configurable banners to be displayed at login
    - Timeouts to terminate administrative sessions after a set period of inactivity
    - Protection of secret keys and passwords
- **Protection of the TSF** - The TOE ensures the authenticity and integrity of software updates through hash comparison and requires administrative intervention prior to the software updates being installed.
- **TOE Access** - Prior to login, the TOE displays a banner with a message configurable by the Security Administrator. The TOE terminates user connections after an Authorized Administrator configurable amount of inactivity time.
- **Trusted path/channels** - The TOE uses TLS to provide a trusted channel between itself and remote syslog and LDAP servers. The TOE uses SSH to provide a trusted path between itself and remote administrators.

5 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 the NDcPP22e should be consulted if there is interest in that material.

6 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e and applicable Technical Decisions 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 only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the *collaborative Protection Profile for Network Devices* and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- 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.

7 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Security Target*, version 1.6, 1/24/2022
- *Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Common Criteria Configuration Guide*, Version 1.4, January 24, 2022

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR and Detailed Test Reports (DTR) for Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1, which are not publicly available. The Assurance Activities Report (AAR) provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. Test activities were conducted at the Acumen test facility in Rockville, MD. For VPX FIPS, testing occurred between February 2021 and September 2021 and on December 3, 2021. Test activities for MPX FIPS occurred between January 20, 2021, and August 26, 2021, and on December 7, 2021. Regression testing for both VPX and MPX was performed from September 26, 2021, through October 23, 2021. Testing to address Validation team comments was performed January 3, 2022, through January 20, 2022.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary DTR and ETR documents. The reader of this document can assume that activities and work units received a passing verdict.

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 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

9.1 Evaluation of Security Target

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 that are consistent with the Common Criteria, and product security function descriptions that support 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 Development Documentation

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance document. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

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 Guidance Documents

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guidance 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 Life Cycle Support Activities

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

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 Test Documentation and the Test Activity

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e and recorded the results in a 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

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Vulnerability Assessment for Citrix ADC (MPX and VPX)*, Version 1.2, January 19, 2022. prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluation team performed multiple public searches for vulnerabilities, with the final search being conducted on January 11, 2022, and did not discover any public issues with the TOE. The keywords used for the search were as follows:

- Citrix ADC 12.1
- Citrix MPX
- Citrix VPX
- MPX 8900 FIPS
- MPX 15000-50G FIPS
- FreeBSD 8.4
- ESXi 6.5
- Dell PowerEdge R630 Server
- Intel Xeon E5-2680 v4
- Intel Xeon Processor E5-2620 v4
- Intel® 8955 Chipset
- TLS
- SSH

- Load Balancer
- TCP
- FreeBSD
- GNU Bash
- GNU Binutils
- GNU gettext
- lrzsz
- lsof (utility to inspect the open file
- Minicom (used by ADC platform)
- monit (daemon to start/stop/monitor services)
- OpenSSL
- PCI Utilities [Used by Platform]
- Precision Time Protocol daemon
- srm (used by platform [secure shell binary])
- zlib
- RRDTOOL

The following resources were used for the searches:

- https://www.citrix.com/products/citrix-adc/
- https://nvd.nist.gov/view/vuln/search
- https://cve.mitre.org/cve
- http://www.kb.cert.org/vuls/html/search
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com/
- https://www.rapid7.com/db/vulnerabilities

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. 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 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 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.

11 Annexes

Not applicable.

12 Security Target

Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Security Target, Version 1.6, 1/24/2022

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

1. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5, April 2017.
3. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5, April 2017.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5, April 2017.
5. *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020
6. *Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Security Target*, Version 1.6, 1/24/2022 [ST]
7. *Assurance Activity Report for Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1*, Version 1.3, 01/24/2022 [AAR]
8. *Evaluation Technical Report for Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1*, Version 1.2, 1/19/2022 [ETR]
9. *Citrix ADC (MPX FIPS and VPX FIPS) Version 12.1 Common Criteria Configuration Guide*, Version 1.4, January 24, 2022 [AGD]
10. *Vulnerability Assessment for Citrix ADC (MPX and VPX)*, Version 1.2, January 19, 2022
11. *Test Plan for Citrix ADC VPX FIPS Version 12.1*, Version 1.4, 1/20/2022 [DTR]
12. *Test Plan for Citrix ADC MPX FIPS Version 12.1*, Version 3.2, 1/20/2022 [DTR]