National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
Dell EMC Networking SmartFabric OS10.5.4

Report Number: CCEVS-VR-VID11338-2023
Dated: September 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 Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lauren Brandt

Linda Morrison

Clare Parran

Michael Smeltzer

Chris Thorpe

Robert Wojcik

Common Criteria Testing Laboratory

Kevin Steiner

Kenji Yoshino

Nhien Truong

Lightship Security USA, Inc.

Table of Contents

1. Executive Summary 1
2. Identification 2
3. Assumptions & Clarification of Scope 4
4. Architectural Information 7
   4.1. TOE Evaluated Configuration 7
   4.2. Physical Boundary 7
   4.3. Required Non-TOE Hardware, Software, and Firmware 8
5. Security Policy 9
   5.1. Protected Communications 9
   5.2. Secure Administration 9
   5.3. Trusted Update 9
   5.4. System Monitoring 9
   5.5. Self-Test 9
   5.6. Identification and Authentication 9
   5.7. Security Audit 10
   5.8. Cryptographic Operations 10
6. Documentation 11
7. IT Product Testing 12
   7.1. Developer Testing 12
   7.2. Evaluation Team Independent Testing 12
   7.3. Evaluated Configuration 12
8. Results of the Evaluation 15
   8.1. Evaluation of Security Target (ASE) 15
   8.2. Evaluation of Development Documentation (ADV) 15
   8.3. Evaluation of Guidance Documents (AGD) 15
   8.4. Evaluation of Life Cycle Support Activities (ALC) 16
   8.5. Evaluation of Test Documentation and the Test Activity (ATE) 16
   8.6. Vulnerability Assessment Activity (VAN) 16
   8.7. Summary of Evaluation Results 17
9. Validator Comments 18
10. Annexes 19

11. Security Target 20
12. Glossary 21
13. Acronym List 23
14. Bibliography 24

List of Tables

Table 1: Evaluation Identifiers 3
Table 2: Assumptions 5
Table 3: TOE Models 8
Table 4: Tools Used for Testing 14
Table 5: Glossary ..... **Error! Bookmark not defined.**
Table 6: Acronyms 23

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Dell EMC Networking SmartFabric OS10.5.4 provided by Dell. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory in Baltimore, MD, United States of America, and was completed in September 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020.

The TOE is Dell EMC Networking SmartFabric OS10.5.4. 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 and successive versions of the ETR. 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). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Security Target 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.

Error! Reference source not found. 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 to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	Dell EMC Networking SmartFabric OS10.5.4
Sponsor and Developer	Dell Technologies, Inc. One Dell Way Round Rock, TX 78682
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020

Item	Identifier
ST	Dell EMC Networking SmartFabric OS10.5.4 Security Target, v2.0
Evaluation Technical Report	Dell EMC Networking SmartFabric OS10.5.4 Evaluation Technical Report, v0.9
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
Evaluation Personnel	Kevin Steiner, Kenji Yoshino, Nhien Truong
CCEVS Validators	Lauren Brandt, Linda Morrison, Clare Parran, Michael Smeltzer, Chris Thorpe, Robert Wojcik

Table 1: Evaluation Identifiers

3. Assumptions & Clarification of Scope

Assumptions

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

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

The assumptions have been reproduced below for convenience but if there is interest in the full Security Problem Definition, the CPP_ND_V2.2E should be consulted.

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

Identifier	Description
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 2: Assumptions

Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2E as described for this TOE in the Security Target. 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 only shows that the evaluated configuration meets the security claims made in accordance with the evaluation activities specified in CPP_ND_V2.2-SD and performed by the Evaluation team
- This evaluation covers only the specific software version 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.

- 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.

4. Architectural Information

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

4.1. TOE Evaluated Configuration

The TOE is a network switch. The TOE is deployed within a network to provide layer 2 and layer 3 network management and interconnectivity functionality. The TOE interfaces within the scope of evaluation are shown in Figure 1.

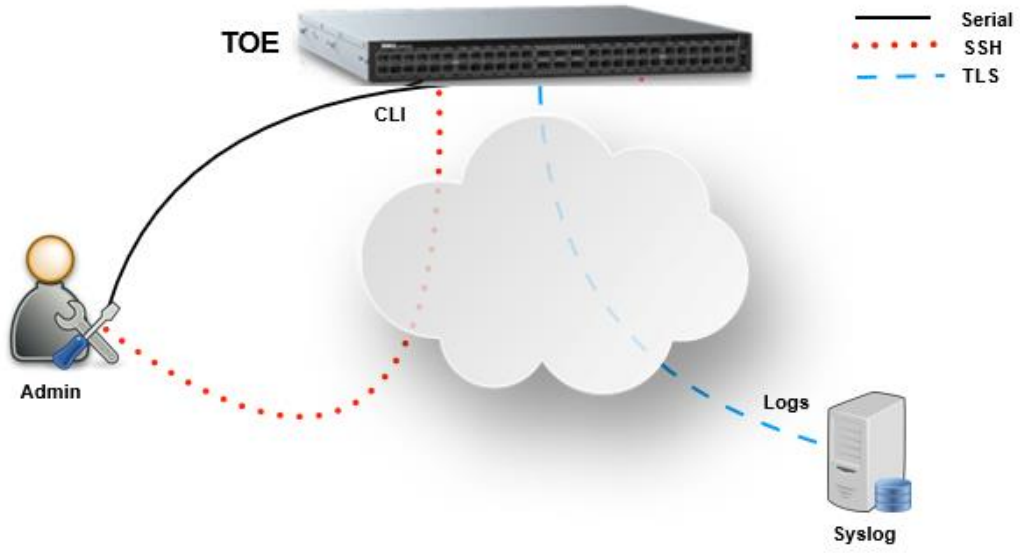

Figure 1: Example TOE deployment

The TOE interfaces are as follows:

- **CLI.** Administrative CLI via direct serial connection or SSH.
- **Logs.** Syslog via TLS.

4.2. Physical Boundary

The physical boundary of the TOE includes all software and hardware shown in Table 3. The TOE is delivered via commercial courier.

Type	Model	CPU	Software	CAVP
Physical	S4112F-ON S4112T-ON S4128F-ON S4128T-ON S4148F-ON S4148T-ON MX5108n	Intel Atom C2338 (Silvermont)	Dell Networking SmartFabric OS 10.5.4	A1949
	MX9116n	Intel Atom C2538 (Silvermont)		
	S5212F-ON N3248TE-ON	Intel Atom C3338 (Goldmont)		
	S5224F-ON S5232F-ON S5248F-ON S5296F-ON Z9264F-ON	Intel Atom C3538 (Goldmont)		
	Z9432F-ON S5448F-ON	Intel Atom C3758 (Goldmont)		
	E3224F-ON	Intel Atom C3558/C3558 R (Goldmont)		
	Z9332F-ON	Intel Pentium D1508 (Broadwell)		

Table 3: TOE Models

4.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- **Audit Server.** The TOE can send audit events to a Syslog server.

5. Security Policy

This section summarizes the security functionality of the TOE:

5.1. Protected Communications

The TOE protects the integrity and confidentiality of communications using TLS and SSH, and using CAVP validated cryptographic algorithms.

5.2. Secure Administration

The TOE enables secure management of its security functions, including:

- Administrator authentication with passwords
- Configurable password policies
- Role Based Access Control
- Access banners
- Management of critical security functions and data
- Protection of cryptographic keys and passwords

5.3. Trusted Update

The TOE ensures the authenticity and integrity of software updates through GPG digital signatures and published hash. The TOE also implements “show version” CLI command that displays information about firmware version running on the TOE. An authorized user must authenticate to the secure Dell Support website where the software downloads are available. The downloaded image must be transferred to the appliance using a secure method such as Secure Copy or SFTP.

5.4. System Monitoring

The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

5.5. Self-Test

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up and generates audit records to record a failure. Self-tests comply with the FIPS 140-2 requirements for self-testing.

5.6. Identification and Authentication

The TOE ensures that all users must be authenticated before accessing its functions and data. TOE can be accessed directly via serial RJ45 connection or remotely via SSHv2 connection. When a user account has sequentially failed authentication the configured number of times, the account will be locked for a Security Administrator defined time period. The TOE uses X.509v3 certificates to support authentication for TLS. Certificate revocation checking is performed using a CRL.

5.7. Security Audit

The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The Security Administrator can configure the TOE to send logs in real-time to a syslog server via TLS.

5.8. Cryptographic Operations

The TOE implements a cryptographic module. The cryptographic module has the ability to generate and destroy cryptographic keys. The cryptographic module uses CAVP validated cryptographic algorithms.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Dell EMC Networking SmartFabric OS10.5.4 Common Criteria Guide*, v1.1
- *Dell SmartFabric OS10 User Guide Release 10.5.4*, 12 2022 Rev. A05

All documentation delivered with the product is relevant to and within the scope of the TOE. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7. IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in the proprietary *Dell EMC Networking SmartFabric OS10.5.4 NDcPPv2.2E Detailed Test Report, Version 0.4,* as summarized in *the Dell EMC Networking SmartFabric OS10.5.4 Assurance Activity Report, v1.2*.

7.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from March 2023 until August 2023. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 2 and **Error! Reference source not found.** below.

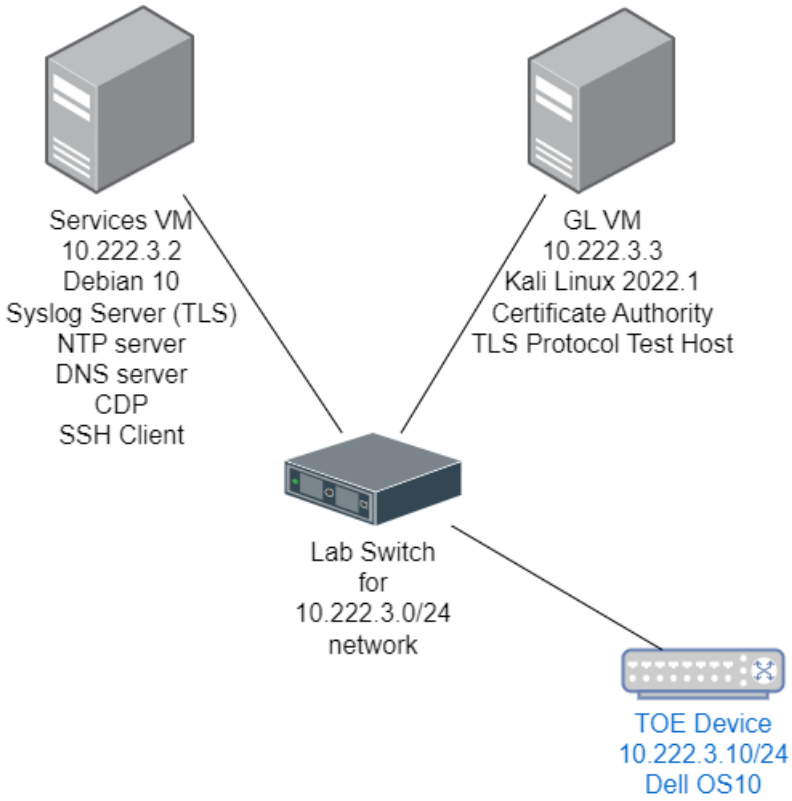

Figure 2: Testing Environment Overview

Name / HW / SW	Description / Functions	Test Tools
Z9432F HW: Z9432F-ON SW: OS10.5.4.3	Fully tested TOE model	N/A
Services VM HW: Test Hypervisor SW: Debian 10	SSH Client (SSH) Perform Packet Captures Syslog Server (TLS) DNS Server CRL Distribution Point	OpenSSH 7.9p1 syslog-ng 3.19.1 dnsmasq 2.80 Wireshark 2.6.20 Python 2.7.16
GL VM Host name: lightship-USCC2203 HW: Test Hypervisor SW: Kali 2022.1	SSH Client (SSH) Protocol Test Host (TLS/SSH) Certification Authority Perform Packet Captures	Greenlight 3.0.34+0 Greenlight 3.0.35 Python 3.9.10 OpenSSL 1.1.1m Wireshark 3.6.0 OpenSSH 8.8p1

Name / HW / SW	Description / Functions	Test Tools
		tcpdump 4.99.1
Test Hypervisor HW: Dell PowerEdge R440 SW: ESXi, 7.0.3	Hosting Services VM and GL VM	N/A
Lab Switch HPE OfficeConnect 1920S Series Switch JL382A	Connect the TOE with the testing environment.	N/A
NETGEAR Switch HW: ProSafe Plus GS105E	Physical disconnect packet captures	N/A
Packet Capture Laptop HW: Lenovo ThinkPad T15 SW: Windows 10 Pro	Physical disconnect packet captures	Wireshark 4.0.4

Table 4: Tools Used for Testing

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined Dell EMC Networking SmartFabric OS10.5.4 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_ND_V2.2-SD.

8.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Dell EMC Networking SmartFabric OS10.5.4 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.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities 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.

8.3. Evaluation of Guidance Documents (AGD)

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

The 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.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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.

8.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities 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.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Dell EMC Networking SmartFabric OS10.5.4 Vulnerability Assessment, Version 1.3, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on August 10, 2023, did not uncover any residual vulnerability.

The Evaluation team searched:

- Common Vulnerabilities and Exposures
    - NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
    - Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
    - CVE Details: https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/plugins
- Tipping Point Zero Day Initiative: https://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/

- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- Dell Security Advisories: https://www.dell.com/support/security/en-us/

The Evaluation team performed a search using the following keywords:

- Dell EMC Networking SmartFabric OS10 Build 10.5.4.3P1
- Each TOE hardware model
- Each processor model used by the TOE
- Linux kernel v4.19.235
- OpenSSL 1.0.2zh
- OpenSSH 8.2
- PKIX-SSH 12.4.3
- Syslog-ng version 3.19.1
- fetch-crl 3.0.19-2

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.

8.7. 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 test activities 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 performed the Evaluation Activities in CPP_ND_V2.2-SD, and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Dell EMC Networking SmartFabric OS10.5.4 Common Criteria Guide*, v1.1 and *Dell SmartFabric OS10 User Guide Release 10.5.4,* 12 2022 Rev. A05. No versions of the TOE and software, either earlier or later, were evaluated. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Customers should be aware that the TOE provides support for IPv6 addresses, however, this functionality is excluded from the evaluated configuration and has not been evaluated. Instructions for disabling IPv6 support can be found in the CC guide.

10. Annexes

Not applicable.

11. Security Target

Dell EMC Networking SmartFabric OS10.5.4 Security Target, v2.0

12. Glossary

Term	Definition
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.
Threat	Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
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.
Vulnerabilities	A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Table 5: Glossary

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

Table 6: Acronyms

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices*, Version 2.2e, 23-March-2020
6. *Evaluation Activities for Network Device cPP*, December-2019, Version 2.2
7. *Dell EMC Networking SmartFabric OS10.5.4 Security Target*, v2.0
8. *Dell EMC Networking SmartFabric OS10.5.4 Common Criteria Guide*, v1.1
9. *Dell SmartFabric OS10 User Guide Release 10.5.4*, 12 2022 Rev. A05
10. *Dell EMC Networking SmartFabric OS10.5.4 Assurance Activity Report*, v1.2
11. *Dell EMC Networking SmartFabric OS10.5.4 Vulnerability Assessment*, Version 1.3
12. *Dell EMC Networking SmartFabric OS10.5.4 Evaluation Technical Report*, v0.9
13. *Dell EMC Networking SmartFabric OS10.5.4 NDcPPv2.2E Detailed Test Report*, Version 0.4
14. *Dell EMC Networking SmartFabric OS10.5.4 NDcPPv2.2E Detailed Test Report Evidence*, Version 0.4