National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Brocade Communications Systems LLC Directors and Switches using FabricOS v9.1.1

Report Number: CCEVS-VR-VID11340-2023
Dated: April 7, 2023
Version: 0.2

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

James J. Donndelinger

Marybeth S. Panock

The Aerospace Corporation

Common Criteria Testing Laboratory

Ryan Hagedorn

Cornelius Haley

Gossamer Security Solutions, Inc.

Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Brocade Directors and Switches using FabricOS v9.1.1 solution provided by Brocade Communications Systems LLC A Broadcom Inc. Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in April 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. 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 Target of Evaluation (TOE) is the Brocade Directors and Switches using FabricOS v9.1.1.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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 Validation Report 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 evaluation technical report 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 Security Target, version 0.5, January 20, 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluated Product	Brocade Directors and Switches using FabricOS v9.1.1 (Specific models identified in Section 8)
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Brocade Directors and Switches using FabricOS v9.1.1 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020
Security Target	Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 Security Target, version 0.5, January 20, 2023
Evaluation Technical Report	Evaluation Technical Report for Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1, version 0.2, March 7, 2023

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
Sponsor & Developer	Brocade Communications Systems LLC A Broadcom Inc. Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
Completion Date	April 3, 2023
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
Evaluation Personnel	Ryan Hagedorn, Gossamer Security Solutions, Inc. Cornelius Haley, Gossamer Security Solutions, Inc. Columbia, MD
Validation Personnel	James Donndelinger: Senior Validator, The Aerospace Corporation Marybeth Panock: Lead Validator. The Aerospace Corporation

3 Assumptions and Clarification of Scope

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

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e 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.

3.2 Clarification of Scope

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.
- Apart from the Admin Guide, additional customer documentation for the specific Router/Switch models 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 NDcPP22e 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.

The Target of Evaluation (TOE) is the Brocade Director and Switch family of products using Fabric OS v9.1.1. The TOE is a family of hardware network devices that create what is called a 'Storage Area Network' or 'SAN'. SANs provide switched connections between servers connected to the SAN and storage devices such as disk storage systems and tape libraries that are also connected to the SAN.

The various models of the TOE differ in performance, form factor and number of ports, but all run the same Fabric OS version 9.1.1 software. The TOE is available in two form factors:

1. a rack-mount Director chassis with a variable number of replaceable modules or 'blades', and
2. a self-contained network switching appliance device

Brocade Directors and Switches are hardware appliances that create a "SAN". SANs enable connectivity between machines in the environment containing a type of network card called a Fibre Channel Host Bus Adapter (HBA) that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment. The network connection between the storage devices in the environment, the TOE, and HBAs in the environment use high-speed network hardware. SANs are optimized to transfer large blocks of data between HBAs and storage devices. SANs can be used to replace or supplement server-attached storage solutions, for example.

HBAs communicate with the TOE using FC or FC over IP (FCIP) protocols. Storage devices in turn are physically connected to the TOE using cabling connected to FC/FCIP interfaces.

4.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

4.2 TOE Architecture

The TOE provides the ability to centralize the location of storage devices in a network in the environment. Instead of attaching disks or tapes to individual hosts in the environment, or for example attaching a disk or tape directly to the network, storage devices can be physically attached to the TOE, which can then be physically attached to HBAs in the environment. HBAs that are connected to the TOE can then read from and write to storage devices that are attached to the TOE according to TOE configuration. Storage devices in the environment appear to the operating system running on the machine that the HBA is installed in as local (i.e. directly-attached) devices.

More than one HBA can share one or more storage devices that are attached to the TOE according to TOE configuration. Scalability is achieved by interconnecting multiple instances

of TOE directors and switches to form a fabric that supports different numbers of HBAs and storage devices.

Directors and switches both can be used by HBAs to access storage devices using the TOE. Switch appliances provide a fixed number of physical interfaces to hosts and storage devices in the environment. Directors provide a configurable number of physical interfaces using a chassis architecture that supports the use of blades that can be installed in and removed from the director chassis according to administrator configuration.

There are administrative interfaces to manage TOE services that can be accessed using an Ethernet network, as well as interfaces that can be accessed using a directly-attached console as follows:

- Ethernet network-based command-line administrator console interfaces – Provides remote command-line administrator console interfaces called the "FabricOS Command Line Interface."
- Serial terminal-based command-line administrator console interfaces – Provides local command-line administrator console interfaces called the "FabricOS Command Line Interface."

There also exists administrative Ethernet network-based programmatic API interfaces that can be protected using TLS; that interface is called a REST API. There exists a modem hardware component that is optional to the product that can be used in a similar manner as a serial console port, but it is disabled by virtue of not being physically installed during initial installation and configuration in the evaluated configuration.

The TOE can operate in either "Native Mode" or "Access Gateway Mode". Only Native mode is supported in the evaluated configuration. Access Gateway mode makes the switch function more like a "port aggregator" and in Access Gateway mode the product does not support the primary access control security functions (mainly zoning) claimed when operating in Native mode.

Separate appliance ports are relied on to physically separate connected HBAs. The appliance's physical location between HBAs and storage devices is relied on to ensure TOE interfaces cannot be bypassed. The TOE encrypts commands sent from terminal applications by administrators using SSH for the command line interface. The TOE requires administrators to login before an SSH session is established

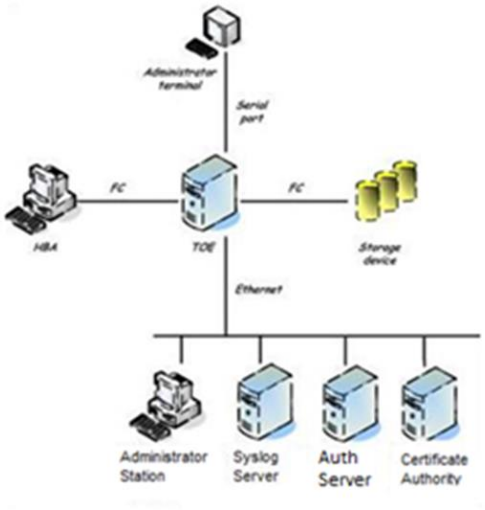

Figure 1: Administrators can access the TOE using a serial terminal or across a network. Audit records are sent to a syslog server.

4.3 Physical Boundaries

The intended environment of the TOE can be described in terms of the following components:

- Host – A system in the environment that uses TOE Storage Area Network (SAN) services.
- Host Bus Adapters (HBAs) – Provides physical network interfaces from host machines in the environment to the TOE. HBA drivers provide operating system interfaces on host machines in the environment to storage devices in the environment. Storage devices in the environment appear to the host operating system as local (i.e. directly-attached) devices.
- Storage device – A device used to store data (e.g. A disk or tape) that is connected to the TOE using a FC/FCIP connection and is accessed by a host using the TOE.
- Terminal application – Provides a runtime environment for console-based (i.e. SSH) client administrator console interfaces.
- NTP Server – Provides network time services to the TOE.
- LDAP Server – Provides authentication support for the TOE.
- Syslog server – Provides logging to record auditable event information generated by the TOE. The syslog server is expected to protect audit information sent to it by the TOE and make that data available to administrators of the TOE.
- Certificate Authority (CA) – Provides digital certificates TLS-based interfaces that are installed during initial TOE configuration. After installation, the CA no longer needs to be on the network for operation.

- Key management systems – Provide life cycle management for all data encryption keys (DEKs) created by the encryption engine. Key management systems are provided by third-party vendors and are not included in the scope of this evaluation.

The TOE relies on a syslog server in the environment to store and protect audit records that are generated by the TOE. The TOE does not rely on any other components in the environment to provide security-related services.

In its most basic form, the TOE in its intended environment of the TOE is depicted in the figure below.

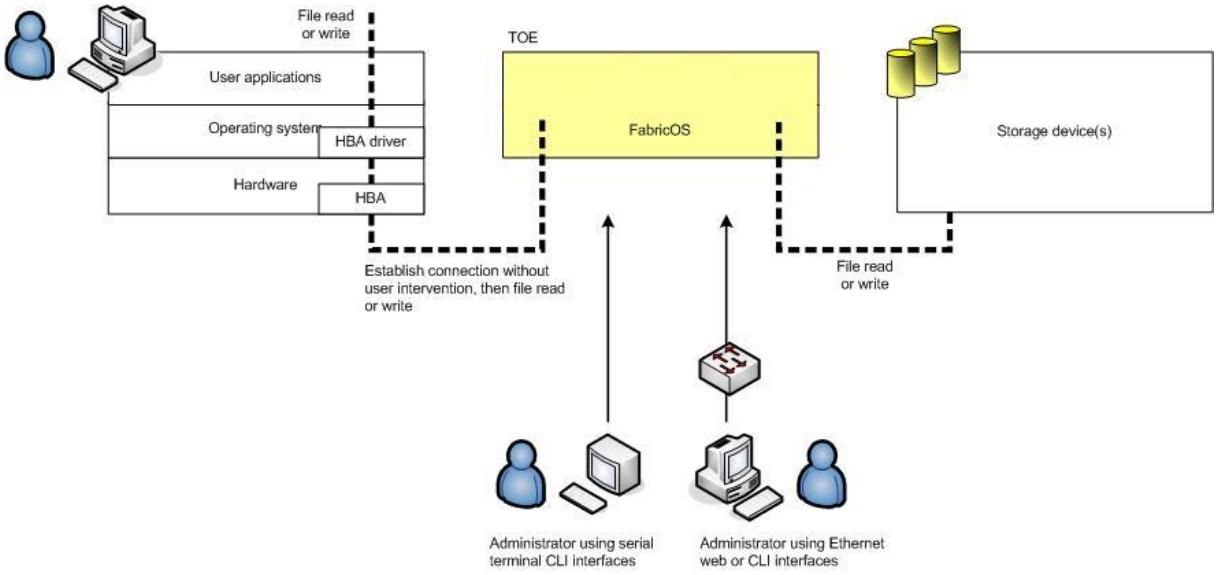

Figure 2: TOE and environment components

5 Security Policy

This section summaries the security functionality of the TOE:

1. Security Audit
2. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access
7. Trusted Path/Channels

5.1 Security Audit

The TOE generates audit events for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware. When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message contents into an encapsulating syslog record.

5.2 Cryptographic Support

The TOE contains CAVP tested cryptographic implementations that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS.

5.3 Identification and Authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. Either the TOE performs the validation of the login credentials or an external authentication server is called.

The TOE provides serial terminal (command line) and Ethernet network-based (command-line) management interfaces. The TOE provides administrative interfaces to set and reset administrator passwords.

5.4 Security Management

The TOE provides both serial terminal- and Ethernet network-based management interfaces. The TOE provides administrative interfaces to configure hard zoning, configure administrative interfaces, as well as to set and reset administrator passwords. By default, host bus adapters do not have access to storage devices.

5.5 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

Note that the TOE is a single appliance, and as such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

5.6 TOE Access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

5.7 Trusted Path/Channels

The TOE enforces a trusted path between the TOE administrators and the TOE using SSH connections for Ethernet connections from the Administrator terminal to the TOE. The TOE encrypts commands sent from terminal applications by administrators using SSH for the command line interface. The TOE provides a TLS protected communication channel between itself and remote audit and authentication servers.

6 Documentation

The following documents were available with the TOE for evaluation:

- Brocade Fabric OS Common Criteria User Guide, 9.1.x, January 19, 2023

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 to 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 developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1, Version 0.2, March 7, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 NDcPP22e including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE consists of the following physical appliances and processors:

Hardware Model	Processor
G720	NXP Semiconductors T1042 (e5500 core)
G730	Intel(R) Atom(TM) CPU C3338R (2cores)
G610	NXP Semiconductors T1042 (e5500 core)
G620	NXP Semiconductors T1042 (e5500 core)
G630	NXP Semiconductors T1042 (e5500 core)
7810	NXP Semiconductors T1042 (e5500 core)
X6-4	NXP Semiconductors P4080 (e500mc core)
X6-8	NXP Semiconductors P4080 (e500mc core)
X7-4	NXP Semiconductors P4080 (e500mc core)
X7-8	NXP Semiconductors P4080 (e500mc core)

The intended environment of the TOE can be described in terms of the following components:

- Host – A system in the environment that uses TOE Storage Area Network (SAN) services.
- Host Bus Adapters (HBAs) – Provides physical network interfaces from host machines in the environment to the TOE. HBA drivers provide operating system interfaces on host machines in the environment to storage devices in the environment. Storage devices in the environment appear to the host operating system as local (i.e. directly-attached) devices.
- Storage device – A device used to store data (e.g. A disk or tape) that is connected to the TOE using a FC/FCIP connection and is accessed by a host using the TOE.
- Terminal application – Provides a runtime environment for console-based (i.e. SSH) client administrator console interfaces.
- NTP Server – Provides network time services to the TOE.
- LDAP Server – Provides authentication support for the TOE.
- Syslog server – Provides logging to record auditable event information generated by the TOE. The syslog server is expected to protect audit information sent to it by the TOE and make that data available to administrators of the TOE.
- Certificate Authority (CA) – Provides digital certificates TLS-based interfaces that are installed during initial TOE configuration. After installation, the CA no longer needs to be on the network for operation.
- Key management systems – Provide life cycle management for all data encryption keys (DEKs) created by the encryption engine. Key management systems are provided by third-party vendors and are not included in the scope of this evaluation.

The TOE relies on a syslog server in the environment to store and protect audit records that are generated by the TOE. The TOE does not rely on any other components in the environment to provide security-related services.

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 ETR. The reader of this document can assume that all assurance 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 Directors and Switches using FabricOS v9.1.1 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

9.1 Evaluation of the 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 Brocade Directors and Switches using FabricOS v9.1.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 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 documents. Additionally the evaluator performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

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

The validator 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 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 validator 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 (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) 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 evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 3/7/2023 with the following search terms: "Brocade", "FabricOS", "Broadcom", "FOS", "TLS", "SSH", "LDAPS", "e5500", "e500mc", "Intel+Atom".

The validator 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 notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in Brocade Fabric OS Common Criteria User Guide, 9.1.x, January 19, 2023. No versions of the TOE and software, either earlier or later were evaluated.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 Security Target, Version 0.5, January 20, 2023*.

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 components, Version 3.1, Revision 5, April 2017.

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

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

[5] collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020.

[6] Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1 Security Target, Version 0.5, January 20, 2023 (ST).

[7] Assurance Activity Report for Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1, Version 0.2, March 7, 2023 (AAR).

[8] Detailed Test Report for Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1, Version 0.2, March 7, 2023 (DTR).

[9] Evaluation Technical Report for Brocade Communications Systems LLC Directors and Switches using Fabric OS v9.1.1, Version 0.2, March 7, 2023 (ETR)

[10] Brocade® Fabric OS® Common Criteria User Guide, 9.1.x User Guide, January 19, 2023