National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Brocade Communications Systems, Inc.

Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00

Report Number: CCEVS-VR-10564-2014
Dated: May 29, 2014
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 solution provided by Brocade Communications Systems, Inc. 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 Catonsville, MD, United States of America, and was completed in Month Year. 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 EAL 1.

The Target of Evaluation (TOE) is the Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 family of products. The TOE is composed of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Brocades' proprietary Multi-Service IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). 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 policies and practices as described on their web site www.niap-ccevs.org.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR and the reports for the ND PP assurance activities. 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 Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 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 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) for Evaluation Assurance Level (EAL) 1 through 4 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
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 (Specific models identified in Section 3.1, below)
Protection Profile	Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) (including the optional SSH and TLS requirements) with Errata #2
ST:	Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 Security Target, Version 1.0, May 19, 2014
Evaluation Technical Report	Evaluation Technical Report for Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00, Version 1.1, May 19, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Brocade Communications Systems, Inc.

Item	**Identifier**
Developer	Brocade Communications Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Patrick Mallett, The MITRE Corporation Brad O'Neill, The MITRE Corporation

3 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 MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 family of products.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Brocades' proprietary Multi-Service IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances.

All TOE appliances are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration (using the Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide) prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. Once configured, the MLX TOE series also offers an encrypted Web Management Interface using TLS.

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations, i.e. PowerPC etc.
- Dynamic memory, used by the central processor for all system operations
- Non-volatile flash memory, used to store the operating system image, startup configuration and other relevant files.
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

3.1 TOE Evaluated Platforms

The Target of Evaluation (TOE) is Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00, including the following series and models:

- Brocade NetIron MLXe Series Hardware Platforms (BR-MLXE-16-MR-M-AC, BR-MLXE-16-MR-M-DC, BR-MLXE-16-MR2-M-AC, BR-MLXE-16-MR2-M-DC, BR-MLXE-8-MR-M-AC, BR-MLXE-8-MR-M-DC, BR-MLXE-8-MR2-M-AC, BR-MLXE-8-MR2-M-DC, BR-MLXE-4-MR-M-AC, BR-MLXE-4-MR-M-DC, BR-MLXE-4-MR2-M-AC, and BR-MLXE-4-MR2-M-DC);
- Brocade NetIron CER 2000 Series Hardware Platforms (NI-CER-2024C-ADVPREM-AC, NI-CER-2024C-ADVPREM-DC, NI-CER-2024F-ADVPREM-AC, NI-CER-2024F-ADVPREM-DC, NI-CER-2048C-ADVPREM-AC, NI-CER-2048C-ADVPREM-DC, NI-CER-2048CX-ADVPREM-AC, NI-CER-2048CX-ADVPREM-DC, NI-CER-2048F-ADVPREM-AC, NI-CER-2048F-ADVPREM-DC, NI-CER-2048FX-ADVPREM-AC, NI-CER-2048FX-ADVPREM-DC, BR-CER-2024C-4X-RT-AC, BR-CER-2024C-4X-RT-DC, BR-CER-2024F-4X-RT-AC, and BR-CER-2024F-4X-RT-DC); and
- Brocade NetIron CES 2000 Series Hardware Platforms (BR-CES-2024C-4X-AC, BR-CES-2024C-4X-DC, BR-CES-2024F-4X-AC, and BR-CES-2024F-4X-DC).

3.2 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance, the Brocade IOS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing functions). IOS enforces applicable security policies on network information flowing through the hardware appliance.

The basic start-up operation of the TOE is as follows:

1. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap.
2. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface, or dropped in accordance with a configured policy.

The TOE will process other packets destined for itself (control path packets) based on the requirements of the given protocol (HTTPS or SSH).

3.3 Physical Boundaries

Each TOE appliance runs a version of the Brocades software and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an external NTP server in the operational environment.

NetIron provides SSL encrypted TACACS+ authentication but does not provide SSL encrypted RADIUS. Thus, the use of RADIUS external authentication services are excluded from the evaluated configuration of the TOE. NetIron’s TACACS+ supports password authentication only and does not support SSH public-key authentication.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security Management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

4.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

4.2 Cryptographic support

The TOE is a FIPS-validated cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature, secure hashing, and key-hashing features in support of higher level cryptographic protocols including SSH and TLS/HTTPS.

4.3 User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various network connections. While implementing applicable network protocols associated with network traffic routing, the TOE is designed to ensure that it doesn't inadvertently reuse data found in network traffic. This is accomplished primarily by controlling the size of all buffers, fully overwriting buffer contents, and zero-padding of memory structures and buffers when necessary.

4.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes.

4.5 Security management

The TOE provides Command Line Interface (CLI) commands and the MLX series provides an HTTPS (utilizing TLS v1.0) Graphical User Interface (Web GUI) to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system.

4.6 Protection of the TSF

The TOE implements a number of features design 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.

4.7 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.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access or, for the MLX series, TLS/HTTPS for Web graphical user interface access. In each case, the both integrity and disclosure protection is ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, the attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata#2. That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide Platform Support: Multi-Service IronWare R05.6.xx, 53-1002735-01, May 19 2014.
- Multi-Service IronWare Administration Configuration Guide Supporting Multi-Service IronWare R05.6.00, 53-1003028-02, 9 December 2013.
- Multi-Service IronWare Security Configuration Guide Supporting Multi-Service IronWare R05.6.00, 53-1003035-02, 9 December 2013

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 Evaluation Team Test Report for the Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00, Version 1.0, February 14, 2014.

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 the Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide Platform Support: Multi-Service IronWare R05.6.xx, 53-1002735-01, 11 February 2014 document and ran the tests specified in the NDPP including the optional SSH and HTTPS/TLS tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 including the following series and models

- Brocade NetIron MLXe Series Hardware Platforms (BR-MLXE-16-MR-M-AC, BR-MLXE-16-MR-M-DC, BR-MLXE-16-MR2-M-AC, BR-MLXE-16-MR2-M-DC, BR-MLXE-8-MR-M-AC, BR-MLXE-8-MR-M-DC, BR-MLXE-8-MR2-M-AC, BR-MLXE-8-MR2-M-DC, BR-MLXE-4-MR-M-AC, BR-MLXE-4-MR-M-DC, BR-MLXE-4-MR2-M-AC, and BR-MLXE-4-MR2-M-DC);
- Brocade NetIron CER 2000 Series Hardware Platforms (NI-CER-2024C-ADVPREM-AC, NI-CER-2024C-ADVPREM-DC, NI-CER-2024F-ADVPREM-AC, NI-CER-2024F-ADVPREM-DC, NI-CER-2048C-ADVPREM-AC, NI-CER-2048C-ADVPREM-DC, NI-CER-2048CX-ADVPREM-AC, NI-CER-2048CX-ADVPREM-DC, NI-CER-2048F-ADVPREM-AC, NI-CER-2048F-ADVPREM-DC, NI-CER-2048FX-ADVPREM-AC, NI-CER-2048FX-ADVPREM-DC, BR-CER-2024C-4X-RT-AC, BR-CER-2024C-4X-RT-DC, BR-CER-2024F-4X-RT-AC, and BR-CER-2024F-4X-RT-DC); and
- Brocade NetIron CES 2000 Series Hardware Platforms (BR-CES-2024C-4X-AC, BR-CES-2024C-4X-DC, BR-CES-2024F-4X-AC, and BR-CES-2024F-4X-DC).

To use the product in the evaluated configuration the image version must be “xmr05600aa” (for the MLX series) or “ce05600aa” (for the CER or CES series). The product also must be configured as specified in the Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide Platform Support: Multi-Service IronWare R05.6.xx, 53-1002735-01, 11 February 2014.

9 Results of the Evaluation

The results of the assurance requirements are summarized in this section. The details of the evaluation results are recorded in the Evaluation Technical Report (proprietary) and Test Summary Report provided by the CCTL. 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 version 3.1 rev 4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Network Devices Protection Profile (NDPP). The evaluation determined that the Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00 TOE to be Part 2 extended, and meets the SARs contained the PP.

The assurance requirements for an evaluation at Evaluation Assurance Level are listed below. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST Introduction
ASE_OBJ.1	Security objectives for the operational environment
ASE_REQ.1	Stated security requirements
ASE_TSS.1	TOE summary specification
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability analysis

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). In order to remain CC compliant, the device(s) must first be configured into FIPS mode, then into Common Criteria mode as specified in the IronWare FIPS and Common Criteria Guide.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Please note further that certain network related functionality is excluded from the approved configuration and that some networking functions relative to the devices were not tested, nor are any claims made relative to their security.

The validators note that "Test 2" in the FCS_TLS_EXT.1 Assurance Activities was not performed. Performance of this test, which is included in the "Security Requirements for Network Devices Errata #2" (dated January 13, 2013), was remove by the TD0004 Technical Decision that is available on the NIAP web site. Annexes
Not applicable

11 Security Target

The Security Target is identified as *Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.6.00, version 1.0, May 19, 2014.*

12 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.

13 **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 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP).