National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Brocade Communications Systems, Inc.
MLX and NetIron CER 2000 Series Router

Report Number: CCEVS-VR-VID10503-2014
Dated: 8 May 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

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jandria S. Alexander (Senior Validator)
James Donndelinger (ECR Chair)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Leidos (formerly SAIC, Inc.)
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Brocade MLX and NetIron CER 2000 Series Router products. The MLX and NetIron CER 2000 Series Router products within the scope of the evaluation comprise the following series and models, all running IOS 5.3:

Brocade MLX 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

BR-MLXE-4-MR2-M-DC

Each of these devices runs the following evaluated software (IOS 5.3), as displayed by the ‘show version’ CLI command:

Boot: Version 5.3.0T165 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

Compiled on Nov 16 2011 at 10:05:30 labeled as xmprm05300

(517880 bytes) from boot flash

Monitor: Version 5.3.0T165 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

Compiled on Nov 16 2011 at 10:04:52 labeled as xmb05300

(524496 bytes) from code flash

IronWare: Version 5.3.0eT163 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

Compiled on Apr 22 2014 at 22:02:40 labeled as xmr05300ea

(8116989 bytes) from Primary

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

Each of these devices runs the following evaluated software (IOS 5.3), as displayed by the 'show version' CLI command:

Boot: Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300

(447585 bytes) from boot flash

Monitor: Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300

(447585 bytes) from code flash

IronWare: Version 5.3.0eT183 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

Compiled on Apr 22 2014 at 22:30:18 labeled as ce05300ea

(14496944 bytes) from Primary.

It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Brocade MLX and NetIron CER 2000 Series Router products was performed by Leidos (formerly Science Applications International Corporation [SAIC]) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in January 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 and assurance activities specified in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is conformant to the *Protection Profile for Network Devices*, Version 1.1, 8 June 2012.

The information in this report is largely derived from the Security Target (ST), the Assurance Activities Report (AAR) and associated test reports. The ST was prepared for Brocade Communications Systems, Inc by Leidos. The AAR and test reports were written by Leidos. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router Security Target. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE family encompasses network devices that provide a security base comprising auditing, cryptographic support for network communications and update integrity, user identification and authentication, and secure management for operational functions related to switching and routing IP network traffic.

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 the 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). 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.

1.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None

International Interpretations

None

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

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 (if any); and
- 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
Target of Evaluation	Brocade MLX 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) with: Boot Version 5.3.0T165, compiled Nov 16 2011 at 10:05:30, labeled as xmprm05300; Monitor Version 5.3.0T165, compiled Nov 16 2011 at 10:04:52, labeled as xmb05300; and IronWare Version 5.3.0eT163, compiled Apr 22 2014 at 22:02:40, labeled as xmr05300ea and 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, and NI-CER-2048FX-ADVPREM-DC) with: Boot Version 5.3.0T185, compiled Nov 16 2011 at 10:06:46, labeled as ceb05300; Monitor Version 5.3.0T185, compiled Nov 16 2011 at 10:06:46, labeled as ceb05300; and IronWare Version 5.3.0eT183, compiled Apr 22 2014 at 22:30:18, labeled as ce05300ea.
Protection Profiles	Protection Profile for Network Devices, Version 1.1, 8 June 2012

Security Target	*Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router Security Target*, Version 1.0, 1 May 2014
Dates of evaluation	November 2012 through May 2014
Assurance Activity Report	*Assurance Activities Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router,* Version 1.2, May 8, 2014
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on November 19, 2012.
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July 2009 and all applicable NIAP and International Interpretations effective on November 19, 2012.
Sponsor	Brocade Communications Systems, Inc., 130 Holger Way, San Jose, CA 95134
Developer	Brocade Communications Systems, Inc., 130 Holger Way, San Jose, CA 95134
Common Criteria Testing Lab	Leidos (formerly SAIC), Columbia, MD
Evaluators	Anthony J. Apted and Dawn Campbell of Leidos
Validation Team	Jandria S. Alexander and Mike Allen of the Aerospace Corporation

3 Security Policy

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

Note: Much of the description of the security policy has been derived from the Brocade Communications System, Inc. MLX and NetIron CER 2000 Router Security Target and Final AAR.

3.1 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 authorized TOE User and also to send the logs to a designated log server using TLS to protect the logs on the network.

3.2 Cryptographic Support

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

3.3 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 does not 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.

3.4 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.

3.5 Security Management

The TOE provides a Command Line Interface (CLI) to access the security management functions used to configure and manage its security functionality. Security management commands are limited to authorized users and available only after they have provided acceptable user identification and authentication data to the TOE.

3.6 Protection of the TOE's Security Functions

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).

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.

3.7 TOE Access Control

The TOE can be configured to display an informative 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.

3.8 Trusted Path/Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access, ensuring both integrity and disclosure protection. 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 external audit servers using TLS connections to prevent unintended disclosure or modification of logs. SSH v2 is used to support SCP which the TOE uses for secure download of TOE updates.

4 Assumptions, Threats, Policies and Clarification of Scope

The assumptions, threats and policies in the following paragraphs were considered during the evaluation of the Lexmark Multi-Function Printers with Hard Drives.

4.1 Assumptions

The ST identifies the following assumptions about the use of the product:

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code.
- A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources.
- A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

4.3 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Clarification of Scope

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, with a certain level of assurance (the assurance activities specified in *Protection Profile for Network Devices* and performed by the evaluation team).

This evaluation covers only the specific device models and 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.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and guidance documentation.

The TOE consists of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Brocade's proprietary Multiservice IronWare Operating System (IOS). The IOS controls the switching and routing of network frames and packets among the connections available on the hardware appliance.

All TOE appliances are configured at the factory with default parameters and an admin and user account with default passwords. Users must login to access the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration 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.

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

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

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.

6 Documentation

The following documentation was supplied by Brocade. The documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

6.1 Product Guidance

The documents listed below are considered to be part of the evaluated TOE. The guidance documentation examined during the course of the evaluation and delivered with the TOE and considered part of the evaluation is as follows:

Brocade MLX Series and NetIron Family Configuration Guide, 53-1002423-02

Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide—Platform Support: Multi-Service IronWare R05.3.xx, 53-1002735-01

Brocade NetIron CES and Brocade NetIron CER Devices Hardware Guide, 53-1002423-02

Brocade MLX Series and Brocade NetIron XMR Hardware Installation Guide, 53-1002424-02

7 IT Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in the following:

- Evaluation Team Test Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Router – MLX Series Hardware Platform
- Evaluation Team Test Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Router – CER 2000 Series Hardware Platform

7.1 Developer Testing

The assurance activities in the Protection Profile for Network Devices do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a test plan based on the Testing Assurance Activities specified in the Protection Profile for Network Devices. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test reports identified above. Tests were executed on the following sample of platforms claimed in the ST:

- BR-MLXE-4-MR2-M-AC hardware platform—all other MLX hardware series platforms included in the TOE are functionally equivalent. The same firmware image is executed on each platform and the only differences are in the numbers (4, 8 or 16) of external physical network connections, the number of management modules (1 or 2) and supported power supplies (AC or DC)
- NI-CER-2024F-ADVPREM-AC hardware platform—all other CER 20xx hardware series platforms listed above are functionally equivalent. The same firmware image is executed on each platform and the only differences are in the numbers (24 or 48) and types (copper or hybrid fiber) of external physical network connections and supported power supplies (AC or DC).

An initial round of testing was conducted the week of May 20, 2013 at the vendor's facility in San Jose, CA. This round of testing identified a number of functional areas where the TOE did not satisfy the requirements specified in the Protection Profile for Network Devices. The developer updated the TOE and subsequent testing took place July 31st, August 1st and August 5th. Final product testing took place on August 20 2013 at the Leidos facility. The developer assisted during the testing phase.

During the final check-out phase of the evaluation, it was identified that there was a vulnerability in the TOE's implementation of TLS, related to certificate validation. The vendor developed a patch to remove the vulnerability and this was tested by the evaluation team on 30 April 2014.

Testing demonstrated the TOE satisfies the security functional requirements specified in the Protection Profile for Network Devices.

The tests performed by the evaluation team and functionality confirmed are summarized as follows:

- The TOE's ability to generate the audit events specified in the ST
- The TOE's ability to establish a trusted channel with an external audit server and transfer audit records to the audit server via the trusted channel
- The TOE supports RSA for public key authentication and password-based authentication over SSH
- The TOE drops an SSH connection if it receives a packet over 256K bytes in length
- The TOE supports SSH connections using AES-CBC-128 and AES-CBC-256
- The TOE does not support DH Group 1 and that it does support DH Group 14
- The TOE supports each of the TLSv1.0 ciphersuites specified in the ST
- The TOE supports the specified password composition requirements, including the specified minimum length
- The TOE provides only obscured feedback when authentication information is entered at the local console
- That for all supported methods of administrator access, the TOE allows access to the CLI when the correct authentication credentials are provided, and denies access when incorrect credentials are provided, and that the services available without authentication are as specified in the ST
- The time could be set by the administrator and synchronized using an external NTP server. Note, the ST does not make any claims about using cryptographic protocols to protect the connection to the NTP server, so testing with the NTP server occurred only over TCP/IP
- That a legitimate update could be installed successfully on the TOE and that an illegitimate update was rejected
- The TOE terminated a remote interactive session after the configured period of inactivity had elapsed. The evaluation team used values of 2, 5, and 8 minutes
- The user was able to terminate both an interactive local session at the TOE console and a remote interactive session over the SSH-provided trusted path
- The TOE terminated a local interactive session after the configured period of inactivity had elapsed. The evaluation team used values of 2, 5, and 8 minutes. Note that the TOE terminates a local interactive session after the inactivity time period has elapsed, rather than locking the session. This is consistent with the selection made in FTA_SSL_EXT.1.1 in the ST

- The TOE displayed a configured notice and consent warning message for each method of access supported by the TOE, i.e., local interactive console, remote interactive SSH using password authentication, and remote interactive SSH using public-key authentication
- The TOE was able to establish a trusted channel with an external syslog server using TLSv1.0. Testing additionally demonstrated the trusted channel was established with the appropriate cryptographic protocol and algorithms to ensure channel data was not sent in plaintext and modification of channel data would be detected by the TOE. A test was also performed to physically interrupt the connection between the TOE and the external syslog server and to verify that communications remained protected when connectivity was restored
- The only method of remote administration for the TOE is via SSH—the evaluation team did not identify any interface that could be used to establish a remote administrative session without invoking the trusted path. Testing additionally demonstrated the trusted path was established with the appropriate cryptographic protocol and algorithms to ensure channel data was not sent in plaintext and modification of channel data would be detected by the TOE.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerabilities applicable to the TOE in its evaluated configuration, but did identify a vulnerability related to another Brocade product (BigIron) with similarities to the TOE. The evaluation team outlined a test for determining if the TOE was susceptible, but analysis of the vulnerability (bypassing ACL rules by using 179 as the source port of a packet) determined it was not relevant as it represents a vulnerability in a TOE capability (packet filtering) that was not subject to evaluation.

8 Evaluated Configuration

The evaluated version of the TOE is Brocade MLX and NetIron CER 2000 Router products with IOS 5.3 including the following series and models:

- Brocade MLX 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
  - BR-MLXE-4-MR2-M-DC
- Each MLX Series device runs the following evaluated software (IOS 5.3), as displayed by the 'show version' CLI command:
  - Boot: Version 5.3.0T165 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

    Compiled on Nov 16 2011 at 10:05:30 labeled as xmprm05300

    (517880 bytes) from boot flash
  - Monitor: Version 5.3.0T165 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

    Compiled on Nov 16 2011 at 10:04:52 labeled as xmb05300

    (524496 bytes) from code flash
  - IronWare: Version 5.3.0eT163 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

    Compiled on Apr 22 2014 at 22:02:40 labeled as xmr05300ea

    (8116989 bytes) from Primary
- 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

- Each NetIron CER Series device runs the following evaluated software (IOS 5.3), as displayed by the 'show version' CLI command:
  - Boot: Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

    Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300

    (447585 bytes) from boot flash
  - Monitor: Version 5.3.0T185 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

    Compiled on Nov 16 2011 at 10:06:46 labeled as ceb05300

    (447585 bytes) from code flash
  - IronWare: Version 5.3.0eT183 Copyright (c) 1996-2009 Brocade Communications Systems, Inc.

    Compiled on Apr 22 2014 at 22:30:18 labeled as ce05300ea

    (14496944 bytes) from Primary.:

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the Protection Profile for Network Devices, Version 1.1, 8 June 2012 (NDPP), in conjunction with version 3.1, revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the NDPP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Routers meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- There are several configuration parameters contained in the ST and highlighted in Section 4.4 above that must be followed to ensure the product is operated in the secure manner required of the evaluated configuration. Failure to follow these guidelines will negate the assurances provided by the evaluation.
- Audit records of TOE activity may be exported to an external entity. Administrators of the product must ensure that there is sufficient storage for these records. In addition, the external audit storage must be protected from unauthorized access and modification or deletion of the audit records.

11 Security Target

The Security Target for this product's evaluation is Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router Security Target, Version 1.0, 1 May 2014.

12 List of Acronyms

AAR	Assurance Activity Report
AES	Advanced Encryption Standard
CBC	Cipher Block Chain
CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
IP	Internet Protocol
IT	Information Technology
MB	MegaByte
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
NVLAP	National Volunteer Laboratory Accreditation Program
PCL	Product Compliant List
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
USB	Universal Serial Bus

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 Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R3, July 2009.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R3, July 2009.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R3, July 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R3, July 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.

[6] Protection Profile for Network Devices, Version 1.1, 8 June 2012.

[7] Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router Security Target, Version 1.0, 1 May 2014.

[8] Evaluation Team Test Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router – CER 2000 Series Hardware Platform, Version 1.0, 1 May 2014.

[9] Evaluation Team Test Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router – MLX Series Hardware Platform, Version 1.0, 1 May 2014.

[10] Assurance Activities Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router, Version 1.2, 8 May 2014.

[11] Evaluation Technical Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router, Part 1 (Non-Proprietary), Version 1.1, 8 May 2014.

[12] Evaluation Technical Report for Brocade Communications Systems, Inc. MLX and NetIron CER 2000 Series Router, Part 2 (Brocade Proprietary), Version 1.0, 30 January 2014.