CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.5.00ca

Maintenance Report Number: CCEVS-VR-VID10543-2014

Date of Activity: 30 May 2014

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 2, September 8, 2008

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 1, February 2004

Impact Analysis Report for Brocade Communications Systems, Inc. Brocade MLXe® and NetIron®Family Devices with Multi-Service IronWare R05.5.00ca, Revision 2.0, 5/29/2014

Brocade Communications Systems, Inc. MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.5.00ca Security Target, Version 1.1, 05/12/2014

Affected Evidence:

Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.5.00c Security Target, version 1.0, December 15, 2013

Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide, 53-1003067-01, 18 November 2013

Multi-Service IronWare Administration Configuration Guide Supporting Multi-Service IronWare R05.5.00, 53-1002818-01, 12 April 2013.

Multi-Service IronWare Security Configuration Guide Supporting Multi-Service IronWare R05.5.00, 53-1002819-01, 12 April 2013.

Multi-Service IronWare Software Upgrade Guide Supporting Multi-Service IronWare R05.5.00, 53-1002826-01, April 12, 2013.

Brocade MLX Series and NetIron Family Documentation Updates Supporting Multi-Service IronWare R05.5.xx, 53-1002673-05, 5 November 2013

Updated Developer Evidence:

Brocade Communications Systems, Inc. Brocade MLXe® and NetIron® Family Devices with Multi-Service IronWare R05.5.00ca Security Target, version 1.1, 05/12/2014

Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide, 53-1003067-01, 19 May 2014

Assurance Continuity Maintenance Report:

Gossamer Laboratories CCTL, on behalf of Brocade Communications Systems Inc., submitted an Impact Analysis Report to CCEVS for approval on May 29, 2014. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence that was updated as a result of those changes, and the security impact of those changes.

Changes to TOE:

The TOE has been revised to perform server certificate validation when acting as a TLS client. The following checks have been added to the TOE:

1. Only RSA certificates will be accepted. [Algorithm Identifier as specified Section 4.1.2.3 of RFC 5280]
2. Public Key should be greater than or equal to 2048 bits. [Subject Public Key Info as specified in Section 4.1.2.7 of RFC 5280]
3. The Signature Algorithm must be using SHA256. [Algorithm Identifier as specified Section 4.1.2.3 of RFC 5280]
4. The Validity fields (Not Valid Before, Not Valid After) must pass the test at the time of use of the certificate. [Validity as specified in Section 4.1.2.5 of RFC 5280]
5. The IP address of the server should be present in the SAN extension field of the certificate. [Subject Alternative Name (SAN) as specified in Section 4.2.1.6 of RFC 5280]. Only Ipv4 addresses will be parsed and considered.
6. The issuer of the certificate should have a self-signed certificate in the trusted certificate list of the FastIron and NetIron device. [Issuer as specified in Section 4.1.2.4 of RFC 5280] For verifying that the issuer is indeed the issuer, we will look for a match in the Key Identifier first and if not present, then on the Distinguished Name.
    a. For Key Identifier match, we look for a match between the Authority Key Identifier of the server's certificate, and the Subject Key Identifier of the issuer's certificate. [Issuer Key Identifier as specified in Section 4.2.1.1, Subject Key Identifier as specified in Section 4.2.1.2 of RFC 5280]

   b. For Distinguished Name match, we look for a match between the Issuer in the server's certificate, and the Subject in the issuer's certificate. [Issuer as specified in Section 4.1.2.4, Subject as specified in Section 4.1.2.6 of RFC 5280]
7. The server's certificate signature should be valid, based on the public key provided in the issuer's self-signed certificate. [signatureValue as specified in Section 4.1.1.3, Subject Public Key Info as specified in Section 4.1.2.7 of RFC 5280]

Vendor Conclusion: The changes consist of the patch to fix the lack of certificate validation by the TOE. The Gossamer evaluation lab witnessed the regression testing of the patch and verified that the patch does indeed address NIAP's concerns.

Note that Brocade continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Validation Team Conclusion: The vendor reports that testing of the specific changes via regression testing was conducted and the evaluation lab witnessed the regression testing of the patch. Supporting evidence was provided in the IAR package. The vendor updated the relevant evidence and configuration guide to reflect the effected changes.

The validation team reviewed the changes and the analysis of the impact upon security, and found that the fix allows the product to operate as described in the Security Target. Therefore the validation team concurs the change is minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6.. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.