CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR BROCADE COMMUNICATIONS SYSTEMS, INC. BROCADE FASTIRON SX, ICX, AND FCX SERIES SWITCH/ROUTER 7.3.00j

Maintenance Update of Brocade Communications Systems, Inc. Brocade FastIron SX, ICX, and FCX Series Switch/Router 7.3.00j

Maintenance Report Number: CCEVS-VR-VID10505-2014a

Date of Activity:	30 May 2014
References:	Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008; Impact Analysis Report for Brocade Communications Systems, Inc. Brocade FastIron SX, ICX, and FCX Series Switch/Router 7.3.00j, Revision 2.0, May 29, 2014

Documentation Updated: (List all documentation updated)

- Brocade Communications Systems, Inc. FastIron SX, ICX, and FCX Series Switch/Router Security Target, v1.1, 5/13/2014.

Assurance Continuity Maintenance Report:

Gossamer Laboratories submitted an Impact Analysis Report (IAR) to CCEVS on behalf of Brocade Communications Systems on 29 May 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 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Changes to TOE:

The TOE has been revised to perform server certificate validation when acting as a TLS client. This revision was a fix made after a vulnerability was identified. The fix supports configuration of the TOE to export audit records to an external SYSLOG server. This communication is protected with the use of TLS. The TLS connection to the Syslog server is configured to meet Security Functional Requirement FTP_ITC.1, which requires that the TOE be configured to use TLS to ensure that any authentication operations and exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification. The following checks have been added to the TOE:

- Only RSA certificates will be accepted. [Algorithm Identifier as specified Section 4.1.2.3 of RFC 5280]
- 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]
- The Signature Algorithm must be using SHA256. [Algorithm Identifier as specified Section 4.1.2.3 of RFC 5280]

- 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]
- 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.
- 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.
    - 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]
    - 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]
- 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]

These changes address the certificate validation check missing in previous versions of the TOE. The vendor performed regression testing to validate that the bug was fixed and this testing was witnessed by the Gossamer Laboratories Common Criteria Test Lab. The test demonstrated the bug fix and that the fix did not impact or change any other TOE functions or operations. Test results were provided as part of the IAR. In addition, the Brocade TLS Server Certificate Validation Feature Specification and Design Implementation was provided for review by the CCEVS validators.

Conclusion:

CCEVS reviewed the description of 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 CCEVS has determined that the change is minor and meets the definition for assurance maintenance as described in Scheme Process #6.