



CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR BROCADE COMMUNICATIONS SYSTEMS, INC. BROCADE FASTIRON ICX SERIES SWITCH/ROUTER 08.0.40

Maintenance Update of Brocade Communications Systems, Inc. Brocade FastIron ICX Series Switch/Router 08.0.40

Maintenance Report Number: CCEVS-VR-VID10604-2016a

Date of Activity: 30 March 2016

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 FastIron ICX Series Switch/Router 08.0.40, Revision 1.2, January 15, 2016

Documentation Updated:

- Brocade Communications Systems, Inc. Brocade FastIron ICX Series Switch/Router 08.0.40 Security Target, v0.6, 01/15/2016.
- FastIron 8.0.40 for Brocade ICX Switches, Release Notes Version 1

Assurance Continuity Maintenance Report:

Gossamer Laboratories submitted an Impact Analysis Report (IAR) to CCEVS on behalf of Brocade Communications Systems on 15 January 2016. 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 updated from the FastIron 8.0.30 to the FastIron 8.0.40 to include the ICX 7450-32ZP hardware appliance and to remove the SX Series, FCX Series, ICX 6610 Series, and the ICX 6450 Series of hardware appliances. Additionally, there were several bug fixes and non-security feature additions included in this update.

The ICX 7450-32ZP hardware appliance was added to the already included ICX 7450 family in the ST. This appliance was added to provide additional port and power configuration options and does not affect security. The SX Series, FCX Series, ICX 6610 Series, and the ICX 6450 Series of hardware appliances are all deprecated models that are being removed since they are no longer being supported.

The features added to the product line are either non-security related or are considered to be outside of the scope of the NDPP evaluation. The following is a list of the feature enhancements included in the updated appliances:

- CLI commands executed on the device are stored in warm memory and are now accessible after a user-executed reload or unexpected reboot.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

- User accounts can be configured to re-enable a locked out user without manual intervention.
- Password encryption services can be configured to encrypt passwords using different encryption types.
- Password entry is now required before modification of a local user password. The user is already required to authenticate in order to issue the change password command so this is simply an added layer of security.
- Aruba's ClearPass External Captive Portal was integrated to provide the means to authenticate clients through an external web server.
- Support for OpenFlow was added.
- DHCP enhancements such as new server options were incorporated.
- Long-distance stacking feature enhancements were added for ICX 7750-48C, ICX 7750-48F, and ICX 7450 (all models).
- SNMP updates were incorporated.

Additional features including Campus Fabric, ERSPAN, Dynamic LACP, Dynamic IP ACLs in web authentication, LLDP and CDP parameters for IP phones using RADIUS attributes, and user-configurable MAC addresses were all added into the TOE but found to be outside of the scope of the evaluation.

A RADIUS over TLS function was also added allowing TLS to secure communications between RADIUS/TCP peers by wrapping the entire RADIUS packet payload into a TLS stream. Though there is an SFR in the NDPP covering this topic, the original evaluation did not include this requirement in the ST which makes it outside of the scope of this evaluation. Brocade intends to include this functionality in future evaluations.

In addition to the new features that were added, there were several security related bugs identified in the appliances. Many of the bugs were fixed to improve service and network protocol function, though none of these bugs affected the requirements in the ST. Among the bugs were several relating to SSH, ACL, VLAN, Telnet, Radsec, port-based authentication, and the web GUI; all of which were found to be outside of the scope of the evaluation. A TLS man in the middle vulnerability (CVE-2014-8730) was found in version 8.0.10 but the vulnerability was already fixed before this version was released. Several denial of service bugs were also fixed even though they were also found to be outside of the scope of the evaluation.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found that the TOE platform added, ICX 7450-32ZP, may be considered equivalent to the evaluated platforms and that there are no concerns with the removal of the SX, FCX, ICX 6610, ICX 6450, and ICX 6450 series included in the previous version of the ST. All other changes including feature updates and bug fixes have also been found to be minor. Therefore, the CCEVS has determined that the overall change is minor and meets the definition for assurance maintenance as described in Scheme Publication #6.