ASSURANCE CONTINUITY MAINTENANCE REPORT FOR CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.90 with IPsec VPN Security

Maintenance Update of CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.90 with IPsec VPN Security

Maintenance Report Number: CCEVS-VR-VID11088-2020

Date of Activity: 16 November 2020

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Impact Analysis Report for CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.90 with IPsec VPN Security, Revision 1.1, 11/10/2020
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

Assurance Continuity Maintenance Report:

The purpose of this document is to summarize and present the Common Criteria Evaluation Validation Scheme's (CCEVS) analysis and findings regarding Assurance Maintenance Continuity for the CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router with IPsec VPN Security upgraded from version 8.0.70 to 8.0.90.

Gossamer Security Solutions submitted an Impact Analysis Report to the CCEVS for approval on 6 October 2020. 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 3.0. In accordance with those requirements, the IAR describes the changes made to the certified Target of Evaluation (TOE), the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consisted of the Security Target (ST), the Supporting Software Release Notes, and the Impact Analysis Report. The ST and Guidance document, via Release notes, were updated.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: CommScope Technologies LLC, Ruckus	The Security Target has been updated to identify the current version.

FastIron ICX 7450 Series Router 8.0.90 with IPsec VPN Security Target, version 0.4, September 3, 2020 **Updated to:** CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.90 with IPsec VPN Security Target, version 0.6, November 10, 2020	
Guidance: Ruckus FastIron FIPS and Common Criteria Configuration Guide, 08.0.90, 27 October 2020 FastIron 08.0.70g for Ruckus ICX Switches Release Notes Version 1, 11 November 2019 FastIron 08.0.80f for Ruckus ICX Switches Release Notes Version 1, 13 April 2020 FastIron 08.0.90g for Ruckus ICX Switches Release Notes Version 1, 28 July 2020	The Guidance has been updated via the Release notes to address the new software version and other non-security relevant features.

Changes to the TOE:

The TOE has been revised from the evaluated FastIron 8.0.70 to FastIron 8.0.90. The changes are described in the Release Notes which are summarized below.

New Feature	Assessment
Unified FastIron Image (UFI) support added.	This is consistent with what was evaluated. The difference is the administrator downloads one file instead of two.
Change in default syslog buffer size. The default value of dynamic syslog messages being logged is increased from 50 to 4,000	The evaluated configuration already had this applied.
no-login keyword addition to the RADIUS server definition.	This addition limits the use of the RADIUS server and does not impact the testing that was performed as part of the evaluation.
Default username and password - The device allows initial access only after using the default local username and password. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change.	The Release Notes explain the administrator will be prompted to create a new password after logging in. Since the administrator is required to change the password, FIA_UAU_EXT.1 is not impacted.
SSH enabled by default.	The evaluated configuration uses SSH, therefore, this has no impact.
SmartZone Management added.	The SmartZone functionality is outside the scope of the NDCPP/VPNGW evaluation and is not in the ST.
MACsec support on the ICX 7850	The NDcPP/VPNGW evaluation did not

	include the 7850 platform.
ICX7150, ICX7250, ICX7750, and ICX7850 Ethernet switches support for long-Reach Multimode (LRM) optics connections.	The NDcPP/VPNGW evaluation did not include the 7150, 7250, 7750 or 7850 platform.
RFC 4560 updates.	RFC 4560 not addressed in an NDCPP/VPNGW evaluation.
Command added to reset device to factory settings.	Command resets the device and does not impact the evaluation results.
Show version for bootcode - Modified command output includes a message which warns about any mismatch with the recommended u-boot version.	This is a functional change and has no impact on the NDCPP/VPNGW evaluation.
SAU licensing was added.	SAU licensing is outside the scope of the NDCPP/VPNGW evaluation
Remote Switched Port Analyzer (RSPAN) was added.	RSPAN is outside the scope of the NDCPP/VPNGW evaluation.
HTTPS image download and configuration download/upload.	HTTPS functionality is outside the scope of the NDCPP/VPNGW evaluation.
The access-list command has been deprecated.	Command was not used during the evaluation so this change has no security impact.
Flexible authentication enhancements added.	All flexible features are outside the scope of the evaluation. The administrator is restricted to the evaluated authentication methods.
ICX 7650 devices can be configured as a Control Bridge (CB) stack or standalone in a Campus Fabric (SPX) system. 1-Gbps SPX links are supported between ICX 7650 or ICX 7750 devices serving as CB units and connected PE units in a Campus Fabric network.	These device models are not in the evaluated configuration.
Port Extender (PE) console authentication redirect.	The PE functionality is outside the scope of the NDCPP/VPNGW evaluation.
Reconfiguring a live Campus Fabric (SPX) LAG via command.	This is functional and outside the scope of the NDCPP/VPNGW evaluation.
ARP inspection entry increase.	ARP functionality is outside the scope of the NDCPP/VPNGW evaluation.
Manifest upgrade.	This functionality uses tftp which is not available in the evaluated configuration.
DHCP upgrades.	DHCP functionality is outside the scope of the NDCPP/VPNGW evaluation.
IP Source Guard scale improvements/enhancements.	IP SourceGuard functionality outside the scope of the NDCPP/VPNGW evaluation
VLAN Enhancements.	VLAN functionality is outside the scope of the NDCPP/VPNGW evaluation
Bridge Protocol Data Unit (BPDU) improved scaling.	BPDU functionality is outside the scope of the NDCPP/VPNGW evaluation

Link Aggregation Control Protocol (LACP) timeout change.	LACP functionality is outside the scope of the NDCPP/VPNGW evaluation
Cloudpath enhancements.	Integration with Cloudpath not included in the NDCPP/VPNGW evaluation.
Increased number of monitor ports .	This is functional and outside the scope of the NDCPP/VPNGW evaluation
Enhancement of tab-based autocomplete.	This is functional and outside the scope of the NDCPP/VPNGW evaluation.
LLDP enabled by default.	LLDP functionality is outside the scope of the NDCPP/VPNGW evaluation
LAG between different default port speeds.	LAG functionality is outside the scope of the NDCPP/VPNGW evaluation
MSTP path-cost configuration.	MSTP functionality is outside the scope of the NDCPP/VPNGW evaluation
TCP MSS Adjustment feature.	Handling of TCP sessions is outside the scope of the NDCPP/VPNGW evaluation
Bidirectional Forwarding Detection (BFD) support added.	This is functional and outside the scope of the NDCPP/VPNGW evaluation
Dynamic Host Configuration Protocol version 6 (DHCPv6) Server configuration.	DHCP is outside the scope of the NDCPP/VPNGW evaluation
Forwarding Profiles.	This is functional and outside the scope of the NDCPP/VPNGW evaluation
IPv6 Neighbor Discovery (ND) Proxy support added.	This is functional and outside the scope of the NDCPP/VPNGW evaluation
Syslog messages for xSTP.	This is an extra audit message and not related to the evaluation.
Packet Statistics Enhancement.	This is functional and outside the scope of the NDCPP/VPNGW evaluation
Stacking Enhancements.	Stacking is outside the scope of the NDCPP/VPNGW evaluation
Multiple S-VLAN Support.	SVLAN functionality is outside the scope of the NDCPP/VPNGW evaluation
BPDU Scaling.	BPDU tunneling is outside the scope of the NDCPP/VPNGW evaluation
PoE Data Link Decoupling and PoE Updates and Related Syslog Messages.	Power management is outside the scope of the NDCPP/VPNGW evaluation
Debug Data Collection.	These are not audit logs and are used for connection issues. These logs are is outside the scope of the NDCPP/VPNGW evaluation.
Link Dampening and Alarms.	Link dampening is outside the scope of the NDCPP/VPNGW evaluation.

Bug Fixes	Assessment
ACL Related bugs.	There are several ACL related bugs. The NDcPP does not address ACL related functionality so these bugs are not security relevant in the context of the NDCPP/VPNGW evaluation.
802.1x Port-based Authentication Related bugs.	There are several 802.1x Port-based Authentication related bugs. The NDcPP does not address 802.1x Port-based Authentication related functionality so these bugs are not security relevant in the context of the NDCPP/VPNGW evaluation.
Accounting feature with RADIUS method is enabled for user login.	This is a functional tracking item and outside the scope of NDCPP/VPNGW.
Authentication, Authorization and Accounting of login feature stops working.	This defect is applicable where only tacacs/radius server does not have a reliable connection. As secure radius has a connection established with a radius server, this defect is not relevant to the NDCPP/VPNGW evaluation. (note: it also restricts access and does not open access)
MAC-based authentication bugs.	MAC-based authentication is outside the scope of NDCPP/VPNGW.
Security vulnerability in web server due to a script.	The web server is not in the NDCPP/VPNGW evaluated configuration.
In FIPS-CC mode, Secure logging / Secure radius server connection establishment would fail.	This defect was introduced after 8.0.70 and fixed before 8.0.80 and hence not relevant to the NDCPP/VPNGW evaluation.
FlexAuth bug.	FlexAuth is not in the NDCPP/VPNGW evaluated configuration so this bug is not an issue.
Pre-provisioned ACL configurations that apply to a PE.	Hotswapping functionality is outside the scope of the NDCPP/VPNGW evaluation.
SSH key files may get lost under defined circumstances.	This is a functional and not a security problem. The SSH key needed to be regenerated but did not create a security issue.
SSH session is abruptly terminated when x11 forwarding is enabled on client with any KEX method	X11 is not in the NDCPP/VPNGW evaluated configuration.
SSH bug fixes for SSH hanging.	This is a functional and not a security problem. The administrator needs to restart the SSH session.
SSH to ICX device connection failure bugs.	This is a functional and not a security problem. The administrator needs to kill the SSH process and restart.
SSH login hang.	This is a functional and not a security problem.

	The administrator simply needs to attempt to log in again.
Recurring reset of the switch when FIPS mode is enabled.	This is a functional and not a security problem and it was fixed.
Other software bug fixes identified in the Release Notes.	These were functional and had no bearing on the security requirements as evaluated.

Regression Testing:

CommScope has performed regression testing on 8.0.7-b (and later), 8.0.80 and 8.0.90. The new platform was included in the 8.0.90 regression testing. There were no changes to any SFR or SAR therefore detailed regression testing was not required.

NIST CAVP Certificates:

The operational environment under which the validated cryptographic algorithm implementation was tested is the same as the operational environment as the changed TOE.

Vulnerability Analysis:

A public search for vulnerabilities that might affect the TOE was performed on October 2, 2020. All vulnerabilities found using the national sites and search terms below have been addressed in the Ruckus FastIron ICX Series Switch/Router 8.0.90 (version of the TOE under Assurance Maintenance).

A search of the following sites was conducted:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net),
- SecurITeam Exploit Search (http://www.securiteam.com),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search), and
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The following key words were each selected for search criteria:

- Ruckus
- FastIron
- Allegro
- Allegrosoft
- openssl crypto
- icx
- ssh
- tls

The vulnerability search returned two results. Those matches were related to other products and did not directly impact the TOE.

Conclusion:

CCEVS reviewed the description of the changes and found the overall impact to be minor. All new features, and bug fixes did not affect any TOE Security Functions. Regression testing was done and was considered adequate based on the types of changes made. Gossamer Security Solutions also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance.

In addition, the operational environment under which the validated cryptographic algorithm implementation was tested is the same as the operational environment as the changed TOE. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE.

Therefore, CCEVS agrees that the original assurance is maintained for the product.