ASSURANCE CONTINUITY MAINTENANCE REPORT FOR CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN Security

---

Maintenance Update of CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN Security

Maintenance Report Number: CCEVS-VR-VID11088-2021

Date of Activity: 17 February 2021

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 8.0.95 with IPsec VPN Security, Revision 1.1, 02/03/2021
- PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, 22 November 2019
    - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (CPP_ND_V2.1)
    - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17 (CFG_NDcPPVPNGW_V1.0)
- FastIron 08.0.95 for Ruckus ICX Switches Release Notes Version 1

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 8.0.90 to 8.0.95.

Gossamer Security Solutions submitted an Impact Analysis Report to the CCEVS for approval on 02 February 2021. 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 FastIron ICX 7450 Series Router 8.0.90 with IPsec VPN Security Target, version 0.6, November 10, 2020 **Updated to:** CommScope Technologies LLC, Ruckus FastIron ICX 7450 Series Router 8.0.95 with IPsec VPN Security Target, version 0.7, January 7, 2021	The Security Target has been updated to identify the current version.
Guidance: Ruckus FastIron FIPS and Common Criteria Configuration Guide, 08.0.95, 31 January 2021 FastIron 08.0.95 for Ruckus ICX Switches Release Notes Version 1	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 8.0.90 to FastIron 8.0.95. The changes are described in the Release Notes which are summarized below.

1. There are several new features that are somewhat related to the SFRs but do not directly impact the requirements.

New Feature Description	Assessment
Default username and password - The device allows initial access only after using the default local username (super) and password (sp-admin). The administrator will be prompted to change the default password after logging in for the 1st time. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change	This is related to FIA_UAU_EXT.1. 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, the requirement is not impacted. This was introduced in the 8.0.90 release but is addressed here since it is in the Release Notes.
Enhanced Show commands	This is related to FMT_SMF.1 but is an enhancement to the commands. The commands already provided enough information to meet the

The output is enhanced for a wide range of Access-list and security feature commands, providing easy access to feature settings	requirement, so this is added information for the administrator.
Added Syslogs that indicate the routing table is full.	This is related to FAU_GEN.1. This is an extra function audit event and not a required event by the VPNGW.
If the NTP server has more than 8 names registered with domain name server and when DNS returns more than 8 names during lookup, ICX might reload.	NTP was evaluated and tested with FCS_NTP_EXT.1. This is an edge case that has been fixed but the evaluation results are still valid as the PP requires 3 servers be configured.

2. Many new non-security features have been added. See the following table for an analysis of each.

New Feature Description	**Assessment**
Users are no longer required to reboot the switch when trying to enable DHCP/DHCP6 snooping, Dynamic ARP inspection etc. ACL-per-port-per-vlan configuration is implicitly enabled and is no longer required to be configured separately.	These functions are outside the scope of the VPNGW evaluation.
MAC Access Control Lists MAC ACLs are introduced to make MAC-based traffic filter usage similar to IPv4 ACLs. MAC ACLs replace the previously supported MAC filters feature. CLI configuration will automatically be converted from MAC filters to MAC ACLs when upgrading from e releases	The VPNGW evaluation did not address MACsec. Additionally, regression testing was performed to ensure evaluated functions operated as expected (same as before)
Source Guard ACLs are introduced to work in conjunction with IP Source Guard (IPSG).	The VPNGW evaluation did not address IP Source Guard. Additionally, regression testing was performed to ensure evaluated functions operated as expected (same as before)
ICX 7850 devices can be configured as a Control Bridge (CB) standalone or stack in an 802.1br (SPX) Campus Fabric configuration.	This device is not in the scope of the VPNGW evaluation.
Nexthop scale enhancements A higher IP nexthop table size is supported for all platforms. For ICX 7850 devices, a new entry has been added to the predefined forwarding profiles. The IP nexthop table size has been added to the redefined forwarding profile for these devices.	This device is not in the scope of the VPNGW evaluation
Unicast and Multicast scale enhancements on the ICX 7850. New forwarding profiles with enhanced unicast and multicast scale numbers are supported in this release	This device is not in the scope of the VPNGW evaluation

For the ICX 7850, the maximum number of FDB table entries has been increased, and four predefined forwarding profiles are now supported.	This device is not in the scope of the VPNGW evaluation
The slow path forwarding of IPv4 and IPv6 multicast data packets is enabled by default for PIM-SM groups and disabled by default for PIM-SSM groups. Default settings for slow path forwarding of IPV4 and IPV6 multicast data packets can be changed by configuration.	This is a functional change and has no impact on the VPNGW evaluation.
The command output for the show ip traffic and show ipv6 traffic commands was modified to show more detailed information for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) statistics.	These commands were not used during the evaluation, so this change has no security impacts.
The DHCP client can now be enabled for a non-default Virtual Ethernet (VE) port. By default, the DHCP client is enabled for the default VE port.	The DHCP client functionality is outside the scope of the VPNGW evaluation
PTP ensures clock synchronization in a packet-based network corrects the latency and time delays. A Transparent Clock (TC) measures the time taken for a PTP event message to transit the device, and provides this information to clocks receiving this PTP event message.	The PTP protocol is outside the scope of the VPNGW evaluation. Additionally, regression testing was performed to ensure evaluated functions operated as expected (same as before)
Port Extender (PE) console authentication - The console on a PE unit in a Campus Fabric network, similar to stack member behavior, redirects to the active controller console and is authenticated using the active controller CB unit user name and password.	The PE functionality is outside the scope of the VPNGW evaluation.
VRF route leaking between different VRFs allows you to share selective route information between different VRFs. Inter-VRF route leaking allows leaking of route prefixes from one VRF instance to another VRF instance on the same physical router, which eliminates the need for external routing.	This is functional and outside the scope of the VPNGW evaluation.
VXLAN support is extended to ICX 7650 and ICX 7850.	These devices are not in the scope of the VPNGW evaluation.

3. There are several bugs identified as being part of the security group that have been fixed. See the following table for an analysis of each.

Bug Description	**Assessment**
ACL Related bugs • CPU usage • Display • SNMP Error messages • ACL name update • BUM logging/port-dampening	Several bugs related to ACLs were fixed. They were all functional in nature and does not impact the permit and deny rules for IPsec testing

• Unexpected reloads • UPnP packets blocking	
802.1x Port-based Authentication Related bugs	There are several 802.1x Port-based Authentication related bugs. The VPNGW does not address 802.1x Port-based Authentication related functionality so these bugs are not security relevant in the context of the VPNGW evaluation.
MAC Port-based Authentication Related bugs	There are several MAC Port-based Authentication related bugs. The VPNGW does not address MAC Port-based Authentication related functionality so these bugs are not security relevant in the context of the VPNGW evaluation.
SSH Bugs	There are several connection dropping related SSH bugs. These are denial of access and not extra access so they are not security relevant.
ICX7450 slot 2 4x10GF ports traffic forwarding failed while having stacking and MACsec configured simultaneously.	MACsec is outside the scope of VPNGW.
DOS attack 'ip tcp burst' and 'ip icmp attack-rate' don't work as expected, when the traffic is destined for subnet broadcast	This DOS issue has been resolved.
When sending TCP packet with TTL as 1 and the destination IP address as unknown, CPU spikes to 99%.	This DOS issue has been resolved
Getting IP address from DHCP server will print this syslog Initiation of request for IP address from DHCP client to server will exchange many packets in the following order client to server ---- Discover server to client --- Offer client to server -- Request server to client - ACK When ACK is received on DHCP snooping trusted port this syslog will be logged	This is functional and outside the scope of the VPNGW evaluation.
If SPX setup receives LLC packet with DSAP and SSAP values 0x8940 or 0x89CB, the packet is looped in the network	This is functional and outside the scope of the VPNGW evaluation
System startup time is incorrect in "sh version" output	This is functional and outside the scope of the VPNGW evaluation.
Pre-provisioned ACL configurations that applies to a PE are not properly applied on that PE during hotswap	Hotswapping functionality is outside the scope of the VPNGW evaluation.
After reloading, client is not able to get the ruckus prompt for Cloudpath webauthentication if	Cloudpath is outside the scope of the VPNGW evaluation.

trust port Lag is applied for webauth. access-switch#sh captive-portal weblogin Configured Captive Portal Profile Details cp-name :weblogin virtual-ip :training.cloudpath.net (0.0.0.0) -->no ip and captive-portal is not reachable virtual-port :443 login-page :/enroll/RuckusWireless-26/ Production/	
Private VLAN port is allowed to be configured in a regular VLAN and vice versa with the following message. "Warning: port <x> in Private VLAN is added to Regular VLAN <y> as Tagged Member	This is functional and outside the scope of the VPNGW evaluation.

These changes are primarily functional in nature and are judged to be minor

Regression Testing:

The new platform was included in the 8.0.95 regression testing by the Vendor. 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 January 26, 2021. All vulnerabilities found using the national sites and search terms below have been addressed in the Ruckus FastIron ICX Series Switch/Router 8.0.95 (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 6 results. All issues 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.