National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec

Report Number: CCEVS-VR-11295-2022
Dated: September 14, 2022
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant
Linda Morrison
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Cody Cummins
Allison Keenan
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec solution provided by Commscope Technologies LLC. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in September 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016.

The TOE is the CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec. The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec Security Target*, version 1.0, September 13, 2022 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec (Specific models identified in Section 4.1)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016
ST	*CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec Security Target*, version 1.0, September 13, 2022
Evaluation Technical Report	*Evaluation Technical Report for CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec*, version 1.1, September 13, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
Sponsor	Commscope Technologies LLC
Developer	Commscope Technologies LLC

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Linda Morrison, Clare Parran

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020
- Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016

That information has not been reproduced here and the NDcPP22e/MACsecEP12 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/MACsecEP12 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and the MACsec Extended Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e/MACsecEP12 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is the CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec family of products.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances.

All TOE appliances are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration (using the Ruckus FastIron FIPS and Common Criteria Configuration Guide) prior to being placed into operation. The CLI is a text-based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. This remote management interface is protected using encryption as explained later in this ST.

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product

4.1 TOE Evaluated Platforms

The evaluated configuration consists of the following series and models:

a. ICX 7550 SKUS with ICX7400-4X10GF Module
b. ICX 7650 SKUS with ICX7400-4X10GF Module
c. ICX 7650-48F
d. ICX 7850-48FS

The different series have differing CPUs as described below:

- The ICX 7550 Series utilizes a Quad-core ARM Cortex A72 (ARMv8-A architecture)
- The ICX 7650 Series utilizes a Quad-core ARM Cortex A57 1.6GHz (ARMv8-A architecture)
- The ICX 7850 Series utilizes a Quad-core ARM Cortex A57 1.6GHz (ARMv8-A architecture)

The TOE utilizes the Firmware crypto library referred to as the RUCKUS-IP-CRYPTO-VER-5.0 running on these processors.

4.2 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance, the IOS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). IOS enforces applicable security policies on network information flowing through the hardware appliance.

On the ICX 7550 SKUS and ICX 7650 SKUS the TOE also provides MACsec support using a pluggable ICX7600-4X10GF hardware module. The ICX 7650-48F and ICX 7850-48FS support MACsec on their base module 10-Gbps ports.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface.

4.3 Physical Boundaries

Each TOE appliance has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in an environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances. This communication is protected by TLS.

The use of a RADIUS authentication server is included the evaluated configuration with communication occurring over a protected TLS channel.

The TOE can be configured to establish a MACsec connection with a MACsec capable peer.

The TOE can be configured to use an NTP server for network time or it can use its own hardware clock.

5 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

5.1 Security audit

The TOE generates logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

5.2 Cryptographic support

The TOE contains a CAVP-tested cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including MACsec, SSH and TLS. The TOE supports SHA1 message digest authentication for NTP servers.

5.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except for passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (usernames, passwords and privilege levels) and to authenticate users against these attributes.

5.4 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled using privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system.

5.5 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). The TOE can also be configured to work with an NTP server for reliable time.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

5.6 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

5.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSH for CLI access to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with network peers, such as a log server and authentication server, using TLS or MACsec connections to prevent unintended disclosure or modification.

6 Documentation

The following documents were available with the TOE for evaluation:

- *RUCKUS FastIron FIPS and Common Criteria Configuration Guide, 09.0.10,* September 1, 2022

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Detailed Test Report for CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACSec*, Version 1.1, September 13, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/MACsecEP12 including the tests associated with optional requirements. The DTR, Section 2 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACsecEP12.

8.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e/MACsecEP12 related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e/MACsecEP12 and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the DTR prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluation team searched the National Vulnerability Database (https://web.nvd.nist.gov/view/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), Offensive Security Exploit Database (https://www.exploit-db.com/) on 8/25/2022 with the following search terms: "CommScope", "Ruckus", "FastIron", "ICX7550", "ICX7650", "ICX7850", "ARM Cortex A72", "ARM Cortex A57", "BCM82756", "RUCKUS-IP-CRYPTO-VER-5.0 ".

The Validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the Evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *RUCKUS FastIron FIPS and Common Criteria Configuration Guide, 09.0.10,* September 1, 2022. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 **Annexes**

Not applicable

11 Security Target

The Security Target is identified as: *CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec Security Target*, Version 1.0, September 13, 2022.

12 Glossary

The following definitions are used throughout this document:

Term	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

Table 2: Glossary

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, September 2102.

[4] collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020

[5] Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016.

[6] *CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec Security Target*, Version 1.0, September 13, 2022 (ST).

[7] *Assurance Activity Report for CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec, Version 1.1*, September 13, 2022 (AAR).

[8] *Detailed Test Report for CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACSec, Version 1.1*, September 13, 2022 (DTR).

[9] *Evaluation Technical Report for CommScope Technologies LLC, Ruckus FastIron ICX Series Switch/Router 9.0.10 with MACsec, Version 1.1*, September 13, 2022 (ETR).