National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Ruckus SmartZone WLAN Controllers & Access Points, R5.1.1.3

Report Number: CCEVS-VR-VID11038-2020
Dated: 04/25/2020
Version: 0.4

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant, Senior Validator
John Butterworth, Lead Validator
Michelle Carlson, ECR Team
Jenn Dotson, ECR Team
Lisa Mitchell, ECR Team
The MITRE Corporation

Common Criteria Testing Laboratory

Gossamer Security Solutions
Catonsville, MD

Table of Contents

1 Executive Summary

The evaluation of Ruckus SmartZone WLAN Controllers & Access Points was performed by Gossamer Security Solutions, in the United States and was completed in April 2020. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Ruckus SmartZone WLAN Controllers & Access Points TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Gossamer Security Solutions determined that the product satisfies evaluation assurance level "EAL 1" as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Ruckus SmartZone WLAN Controllers & Access Points, R5.1.1.3 (NDcPP21/WLANASEP10) Security Target, Version 1.0, 04/24/2020.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of Ruckus SmartZone WLAN Controllers & Access Points by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Ruckus SmartZone WLAN Controllers & Access Points, R5.1.1.3 (NDcPP21/WLANASEP10) Security Target, version 1.0, 04/24/2020* produced by Gossamer Security Solutions.

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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Ruckus SmartZone WLAN Controllers & Access Points
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015
ST	Ruckus SmartZone WLAN Controllers & Access Points , R5.1.1.3 (NDcPP21/WLANASEP10) Security Target, version 1.0, 04/24/2020
Evaluation Technical Report	Evaluation Technical Report for Ruckus SmartZone WLAN Controllers & Access Points, version 0.3, 04/24/2020
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	Ruckus Wireless, Inc.
Developer	Ruckus Wireless, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	

3 Architectural Information

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

The Target of Evaluation (TOE) is the Ruckus SmartZone WLAN Controllers & Access Points. Ruckus Wireless Controller has been designed to eliminate the difficulties administrators experience with building and managing large-scale WLAN networks, to support several Wi-Fi access points and many concurrent Wi-Fi clients. Ruckus Wireless Controllers can support tens of thousands of Ruckus Smart Wi-Fi APs and hundreds of thousands of concurrent Wi-Fi subscribers. The Ruckus carrier-class management system provides feature-rich management of access points, such as RF management, load balancing, adaptive meshing and backhaul optimization and secure connectivity to all wireless clients.

3.1 TOE Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The Ruckus SmartZone controllers and Access points Solution (TOE) is a Wireless LAN access system (WLAN). The Wireless LAN access system defined in this ST is composed of multiple products operating together to provide secure wireless access to a wired and wireless network. The TOE provides end-to end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement. The TOE has the following Access Point TOE components: R610, R710, R720, T610 and T710. The TOE also has the following Wireless Controllers: SmartZone 100 (SZ-104 and SZ-124), SmartZone 300 (SZ 300), virtual SmartZone (vSZ-E and vSZ-H hosted on VMware ESXi 6.5), and virtual SmartZone – Data plane (vSZ-D hosted on VMware ESXi 6.5).

Ruckus Wireless Controllers and Ruckus Smart Wi-Fi APs are deployed in a centralized deployment model.

CENTRALIZED DEPLOYMENT MODEL

In a centralized deployment model client traffic always reaches the WLAN controller first via the AP before going to intended destination. See figure 1 and 2.

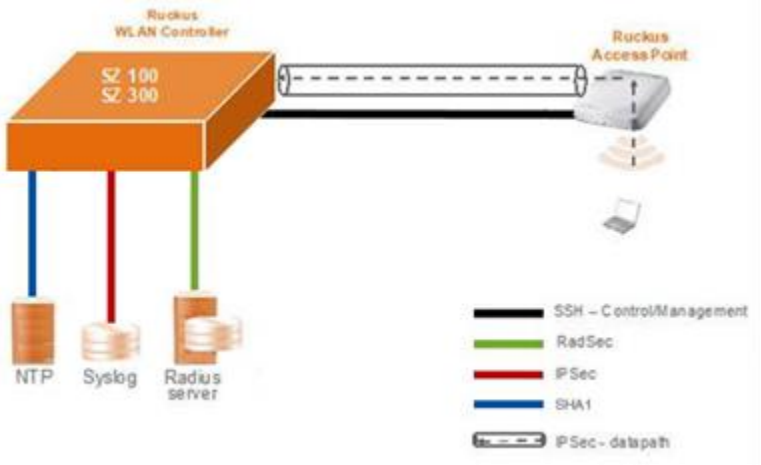

Figure 1 Centralized Deployment with Hardware

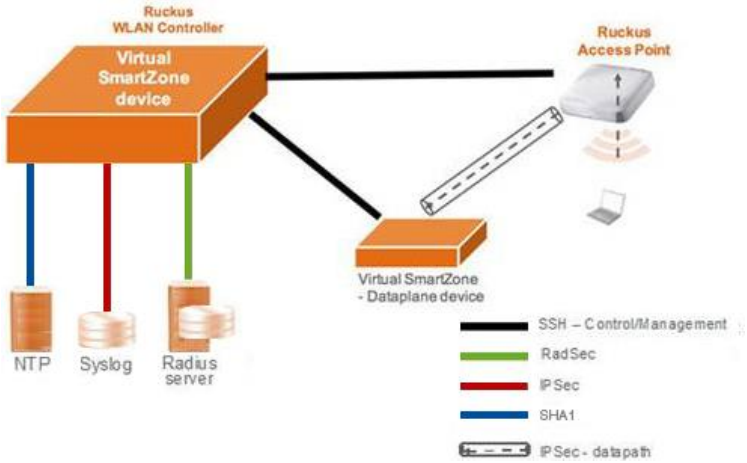

Figure 2 Centralized Deployment with Software

In Figure 1, the physical appliances consist of a Controller and an Access Point (AP) with the Dataplane (DP) built into the Controller. In Figure 2, the virtual deployment has a Controller, a separate DP and an AP.

Once authenticated as trusted nodes on the wired infrastructure, the access points provide the encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the wireless controller for management purposes. The management traffic between Ruckus AP and Ruckus Wireless Controller is encrypted.

3.3 Physical Boundaries

The physical boundaries of the TOE consist of Wireless Controller and Access Points running software version 5.1.1.3.

The specific hardware information is as follows:

Controller	CPU
Smart Zone 100 (includes SZ-104 and SZ-124 models)	IntelCore i7-3770 CPU @ 3.40GHz with AES-NI
Smart Zone 300 (SZ 300)	Intel Xeon CPU E5-2695 v3 @ 2.30GHz with AES-NI
Ruckus virtual SmartZone (includes vSZ-E and vSZ-H) on VMware ESXi 6.5	Intel Xeon CPU E5-2620 v4 @ 2.10GHz with AES-NI
Ruckus virtual SmartZone – Data plane (vSZ-D) on VMware ESXi 6.5	Intel Xeon CPU E5-2620 v4 @ 2.10GHz with AES-NI

Table 1 Controller CPU Identification

AP	CPU
R610	Qualcomm IPQ8064
R710/T610/T710	Qualcomm IPQ8068
R720	Qualcomm IPQ8065

Table 2 AP CPU Identification

The wireless controller serves client devices using secure authentication protocols, such as 802.1X/EAP. This is combined with policy-based data traffic steering which enterprises can optimize to forward all client traffic appropriately.

The wireless controller can function as a very large-scale WLAN controller that can manage a lot of access points, providing feature-rich management including control over their self-organizing smart networking behaviors such as RF management, load balancing, adaptive meshing, and backhaul optimization.

SZ 100
SmartZone™ 100 (SZ-104 and SZ-124) is a Scalable, Resilient, and High Performing Wireless LAN controller for Enterprises. It manages up to 1,024 Wi-Fi access points, 2,000 WLANs, and 25,000 clients per device. SmartZoneOS' unique architecture enables SZ 100 to be deployed in multiple architectures like centralized and distributed traffic forwarding.

SZ 300
The SmartZone™ 300 (SZ 300) Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The SZ300 supports up to 10,000 AP and 100,000 Clients per unit.

vSZ
The Ruckus Virtual SmartZone™ (vSZ-E and vSZ-H hosted on VMware ESXi 6.5) is an NFV-based WLAN controller scale.

vSZ-D
With the Virtual SmartZone Data Plane (vSZ-D hosted on VMware ESXi 6.5), the Ruckus Virtual SmartZone platform launches sophisticated data plane capabilities that enable tunneled WLAN architectures.

The AP components can be centrally managed by the Ruckus Wireless Controller as part of a unified indoor/outdoor wireless LAN. Each AP supports a wide range of value-added applications.

Wireless communications between clients and APs is carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation, the APs use a variation within 802.11a, 802.11ac, 802.11b, 802.11g and 802.11n for wireless communication. The wireless security protocols that are to be used with the APs are 802.1X/802.1i.

The AP part of the TOE consists of the following component products:

AP	Location Type	Concurrent Users	User Data Rate
R610	Medium density	512	Up to 1300 Mbps
R710	High density	512	Up to 1733 Mbps
R720	High density		Up to 1733 Mbps
T610 (including T610S)	Medium density outdoor	512	Up to 1733 Mbps
T710 (including T710S)	High density outdoor	512	Up to 1733 Mbps

Note that the T610S and T710S are the 120 degree sector antenna variants of the T610 and T710 respectively and include all of the same physical features.

4 Security Policy

The TOE enforces the following security policies as described in the ST:

- Security audit
- Communication
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

4.1 Security audit

The TOE provides auditing capabilities to provide a secure and reliable way to trace all changes to the system. Any configuration changes, administrative activities and other auditable events are audited both internally and externally over a secure communication channel to an audit server. All audited events have the necessary details like timestamp, event log, event code, and identity of the party involved to provide a comprehensive audit trail.

4.2 Communication

The distributed TOE offers secure internal TSF communication. Access Points and vSZ-Ds register to the WLAN controller over a dedicated channel and must be approved by the administrator to communicate with each other as parts of the distributed TOE.

4.3 Cryptographic support

The distributed TOE provides cryptographic functions for secure administration access via HTTPS and SSH; for communication between the distributed parts of the TOE via SSH and IPSec; for wireless communication via WPA2 and for communication to external systems such as audit log servers via IPSec and RADIUS via TLS. Functions include key generation, key establishment, key distribution, key destruction, cryptographic operations.

4.4 Identification and authentication

The distributed TOE provides secure connectivity to the network for wireless clients via 802.1X authentication. Certificate-based authentication is supported via external RADIUS server and password-based authentication is supported via the local authentication mechanism. The distributed TOE provides secure password-based authentication for remote administrators and X.509 certificate-based authentication for TOE components. The distributed TOE also provides strong password requirements that can be configured by the administrator including length, session timeout and password complexity. Consecutive unsuccessful attempts beyond a certain limit will result in locking out the user for a specified duration of time.

4.5 Security management

TOE administrators manage the security functions of the TOE's distributed components from the SmartZone Controller, including software updates, via secure HTTPS connection over a web interface. Optionally SSH and the local console can also be used as a method to configure the system via the SmartZone controller. Administration cannot be performed from a wireless client. The TOE also provides the ability to configure the session activity timeout of an administrator and to configure the access banner on the controller.

4.6 Protection of the TSF

The TOE provides image integrity verification to validate the authenticity of the images before loading them. Upon every boot up, power on self-tests are conducted to validate the integrity of the software components. If power up self-tests fail, a quarantine state is entered. All the components of the distributed TOE use X.509 certificates to authenticate and establish a secure connectivity amongst them. The TOE also allows configuration of timestamps via an NTP server. The TOE protects cryptographic keys and passwords from unauthorized access.

4.7 TOE access

A login banner is offered which provides the ability to have a custom warning/access policy message as per the organization needs. The TOE is capable of restricting wireless access based on TOE interface, time and day. The TOE provides the ability to configure an inactivity timeout which terminates the session beyond the inactivity period configured. An administrator can also terminate their own session.

4.8 Trusted path/channels

The TOE communicates to external components in a secure manner. The following secure channels are used to communicate externally – TLS for RADIUS, HTTPS for WebUI administration, SSH for CLI administration, IPsec for audit servers, and WPA2 for wireless clients. The registration and joining of TOE components is performed over a dedicated channel. After registration, SSH is used for all management of the distributed TOE components (AP and vSZ-D) by the SmartZone Controller and IPSec is used for the data tunnel.

5 Assumptions

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

- collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 (NDcPP21)
- Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015 (WLANASEP10)

That information has not been reproduced here and the NDcPP21 and WLANASEP10 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 NDcPP21 and WLANASEP10 as described for this TOE in the Security Target. 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.

5.1 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 Protection Profile for Network Devices and Extended Package Wireless Local Area Network (WLAN) Access Systems 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.
- 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 NDcPP21 and WLANASEP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE (note that the first is Common Criteria specific and is normative while the others are generally informative) is as follows:

- Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and APs,5.1.1.3, Part Number: 800-72111-001 Rev D, April 2020

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the RUCKUS SmartZone WLAN Controllers & Access Points, R5.1.1.3 Assurance Activity Report (NDcPP21/WLANASEP10), Version 0.3, 04/24/2020 (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 a Common Criteria Certification document and ran the tests specified in the NDcPP21 and WLANASEP10 including the tests associated with optional requirements.

8 Evaluated Configuration

The evaluated configuration consists of the following models:

- Wireless Controllers:
    - Smart Zone 100 (includes SZ-104 and SZ-124 models)
    - Smart Zone 300 (SZ 300)
    - Ruckus virtual SmartZone (includes vSZ-E and vSZ-H) on VMware ESXi 6.5
    - Ruckus virtual SmartZone – Data plane (vSZ-D) on VMware ESXi 6.5
- Access Points:
    - R610
    - R710
    - R720
    - T610 (including T610S)
    - T710 (including T710S)

9 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 Ruckus SmartZone WLAN Controllers & Access Points TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21 and WLANASEP10.

9.1 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 Ruckus SmartZone controllers and Access points Solution products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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.

9.2 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 NDcPP21/WLANASEP10 related to the examination of the information contained in the TSS.

The validator 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.

9.3 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 of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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.

9.4 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 validator 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.

9.5 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 NDcPP21/WLANASEP10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. Neither the public search for vulnerabilities nor the fuzz testing uncovered any residual vulnerability.

The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- 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 Engin (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/)

The search was performed on 4/5/2020 with the following search terms: "router", "switch", "TCP", "IPsec", "TLS", "SSH", "RadSec", "802.1X", "Ruckus", "SmartZone", and "ESXi".

The validator 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.

9.7 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.

10 Validator Comments/Recommendations

The validation team recommends that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The validation team recommends the consumer pay attention to the password complexity recommendations provided in the vendor guidance documentation in the Password Management section. There is no password complexity enforcement other than length, so it is up to the consumer/administrator to self-impose password complexity.

The validation team recommends that consumers deploy these devices as recommended by the vendor in their guidance documentation. For example, in section AP Configuration in FIPS Mode in the guidance, the vendor advises the registration of TOE components be performed in a "controlled environment in which there is a segregated network with only TOE components present."

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: Ruckus SmartZone WLAN Controllers & Access Points (NDcPP21/WLANASEP10) Security Target, Version 1.0, 04/24/2020.

13 Glossary

The following definitions are used throughout this document:

- **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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019 (NDcPP21)

[6] Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 29 May 2015 (WLANASEP10)

[7] Ruckus SmartZone WLAN Controllers & Access Points, R5.1.1.3 (NDcPP21/WLANASEP10) Security Target, Version 1.0, 04/24/2020.

[8] Ruckus SmartZone WLAN Controllers & Access Points, R5.1.1.3 Assurance Activity Report (NDcPP21/WLANASEP10), Version 0.3, 04/24/2020 (AAR).

[9] Detailed Test Report (NDcPP21/WLANASEP10) for Ruckus SmartZone WLAN Controllers & Access Points, Version 1.1, 04/24/2020 (DTR).

[10] Evaluation Technical Report (NDcPP21/WLANASEP10) for Ruckus SmartZone WLAN Controllers & Access Points, Version 0.3, 04/24/2020 (ETR)