Ruckus Networks - Security Advisory

ID 20180427 FAQ

SmartZone Security Best Practices

Initial Internal Release Date: **04/27/2018**
Initial Release to the public***: 04*/27/2018**
Update Release Date: **04/27/2018**

PRELUDE:

Recently, a few SmartZone customers reported that their controllers were experiencing abnormally high CPU usage. On analysis, Ruckus discovered these controllers were undesirably exposed to the internet without any Firewall protection. The controllers were found to be infected with malware, which got in, by exploiting Java JMX/RMI security vulnerabilities. Ruckus team worked with the impacted customers to eliminate the malware and provided the software patches to make sure they are completely immune against any kind of attack. These attacks are declared as "HIGH" risk.

Ruckus Networks Response (Mechanisms, techniques and best practices to achieve Smart-Zone network security):

Ruckus Networks understands the risks and potential threats posed to SmartZone customers in general and have many mechanisms in place to avoid and thwart these attacks.

The Wifi network typically consists of below components namely:
- **WiFi devices** - laptops, smartphones, tablets etc brought in by clients
- **Access Points** - last mile where the user/client device connects
- **Controllers** - Appliance and cloud based solutions required to manage the APs as well as the clients /devices connected to them
- **Other miscellaneous services** - DHCP, DNS, Radius servers, Firewalls etc

To achieve end-to-end security, all the above components need to be monitored and secured. Below are some of the mechanisms and compliance controls in place for the Ruckus Wireless Access Points and Controllers.

1. The Ruckus Wireless APs are one of the most secure Access Points in the industry, where AP firmware undergo various functional, stress and security scan tests before we publish to the customers. The Access Point firmware is digitally signed using PKI infra-structure and any tampering of the AP firmware/software is completely ruled out.

2. AP and Controller firmware are periodically subjected to security scans to find any secu-rity vulnerabilities in the software. In case of any vulnerability is reported, appropriate steps are taken to fix these vulnerabilities and again re-scan till the report comes out

completely clean.

3. The Quality Assurance teams deploy manual and tool assisted testing methodologies to find any security vulnerabilities and fix them prior to any General Availability (GA) release.

4. Both APs and Controllers use Linux as operating system. Since most of the vulnerabilities related to Linux OS are reported and fixed by distribution vendors, Ruckus Wireless keeps track of the security bulletins of these distribution and security fixes are patched to our firmware as made available by vendors. The patch information is released as security advisory and details of the fixes / workaround is available at our public portal https://www.ruckuswireless.com/security and https://support.ruckuswireless.com/security

5. Most of the security, encryption and decryption software used by AP and controller firmware is also provided by open source community (e.g. Openssl, OpenSSH etc), which are robustly tested for the vulnerabilities. These well know communities provide the vulnerability information and corresponding fixes on their public portals on regular basis. Ruckus Wireless security team (SIRT) actively monitors these publications and provide swiftest actions on providing information on all zero day vulnerabilities with advisories. We also ensure that fixes, workaround and patches are available in shortest response time to most of the active software releases. The patch information is released as security advisory and details of the fixes / workaround is available at our public portal https://www.ruckuswireless.com/security and https://support.ruckuswireless.com/security

6. All the communication between the Ruckus Wireless components (AP, SZ etc) is via secure tunnels namely (SSH, Ruckus GRE). We make sure that the latest SSL versions (e.g. TLSv1.1, 1.2 etc) are used during the tunnel establishment phase and all the industry recommended best practices for the secure tunneling.

7. For Captive portal based WLANs, use SSL/TLS based portals for login and landing pages and all the HTTP GET and POST request should be encrypted. Also the client VLANs should be configured for these WLANs which help to partition the network and reduce and limit the extent of damage in case of attacks.

8. If non-captive portal based WLAN/SSIDs are used then it is recommended to use Ruckus Wireless Proprietary DPSK which assigns different passphrase to different users and provides better security than normal PSK based WLAN.

9. Default SSID names should never be used and custom names should be configured.

10. Always enable 802.11r fast roaming feature for secure roaming.

11. Always enable Ruckus Proprietary client isolation feature on WLANs to avoid peer to peer attacks.

12. Always enable Ruckus Proprietary Force DHCP feature on WLANs to avoid any DHCP spoofing.

13. Always enable Ruckus Proprietary Proxy ARP feature to avoid ARP spoofing attacks.

14. Always enable Ruckus Proprietary Rouge AP detection feature to avoid Rouge APs and Evil Twin attacks.

15. Always enable Ruckus Proprietary DoS protection feature for Rouge clients to avoid DoS attacks.

The following are SmartZone specific recommendations.

1. Ruckus SmartZone products must be placed in the DMZ behind a Firewall.

2. The firewall should block the following JMX/RMI ports to render these inaccessible from the internet: 7199, 10103, 10112, 10113, 10116, 10117, 10118, 10119, 10120, 11001.

3. Please check for the latest security bulletins at www.ruckuswireless.com/security and upgrade to latest firmware and patches posted here.

In view of industry's reported crypto hijacking and other attacks, the above Security Best Practices are strongly recommended.

What is the impact on Ruckus products?
Ruckus SmartZone products prior to Release 3.6.1 are impacted.

When will this Ruckus Security Advisory be publicly posted?
Ruckus Wireless released the initial security advisory to Ruckus field teams on: 04/27/2018
Ruckus Wireless released the initial security advisory to customers on: 04/27/2018
Public posting: 04/27/2018

Revision History

Version	ID	Change	Date
1.0	20180427	Initial Release	April 27, 2018

Ruckus Support can be contacted as follows:

The full contact list is at: https://support.ruckuswireless.com/contact-us

DISCLAIMER