Ruckus Wireless Security Advisory ID 080216 FAQ:

Vulnerabilities in WebGUI Interface on Ruckus Unmanaged-APs

Internal Release Date: **08/02/2016**
Release to the public**: 08/02/2016**
This Ruckus Security Advisory constitutes Ruckus Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Wireless.

What are the issues?

Multiple vulnerabilities were found in the WebGUI interface of Ruckus APs. These vulnerabilities were first reported by Tripwire and Ruckus acknowledges them. The vulnerabilities can be broadly classified into two categories: 1. CSRF exposure, 2. Un-authenticated command injection and information retrieval sometimes causing denial of service attack on AP.

However Ruckus would like to state that these vulnerabilities are only exploitable when AP IP & Web interface are accessible from external hosts. Most of Ruckus APs are deployed in managed environment where there is WLAN controller that is managing the APs. In this mode of operation the Web interface is not enabled and in most cases even the IP address of the AP is not reachable from external sources. This prevents from these vulnerabilities from getting exploited.

We do acknowledge that in deployments where AP IP and Web interface are accessible from external sources, these vulnerabilities can be exploited causing disruption of service. To prevent this we recommend the following precautions.

- If AP Web interface access is not required for managing the AP, then it should be disabled by configuration. This can be done through AP CLI.
- If access to Web interface is required but IP level access can be limited to internal network only, then access to IP from external sources should be prevented through Firewall policies.
- If AP needs to be accessed over Internet and Web interface access required, then Firewall policies should be added to limit this access only to authorized IPs.

With these precautions the unmanaged-APs can be protected from exploitation of these vulnerabilities.

Ruckus will be actively working to close these vulnerabilities with high priority. Timelines for software release with these vulnerabilities fixed along with release details will be announced through updated versions of this advisory.

What is the impact of this for other Ruckus products?

All Ruckus APs are vulnerable when the Web interface is accessible from external sources except unleashed product line. Unleashed AP models are not vulnerable to un-authenticated command injection issue on the Web interface.

SZ/SCG and ZD product line is only vulnerable to CSRF. It is not vulnerable to un-authenticate command injection issue on the Web interface.

How do I check if I am vulnerable?

To check if the AP Web interface is vulnerable in your setup, attempt to access the IP address of AP from a host on external network over HTTP/HTTPS. If the AP comes back with an admin login, then the AP is vulnerable.

What workaround can I apply?

If the Web interface is not required, simply go to AP CLI and disable the HTTP and HTTPS interfaces. If the Web interface access is required, then install the Firewall rules in the Firewall protecting the network and repeat the test.

How does Ruckus Wireless qualify severity of security issues?

Ruckus Wireless typically utilizes the Common Vulnerability Scoring System (CVSS) v3. However for

these issues the severity is being analyzed, we will publish as soon we complete and have preliminary severity data.

When will this Ruckus Wireless Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: **08/02/2016**

Ruckus Wireless released the initial security advisory to customers on: **08/02/2016**

Public posting: **08/02/2016**

Version: Initial Release 1.0

Ruckus Support can be contacted as follows:

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