ID 062117 FAQ

Vulnerabilities in Web GUI Interface on Ruckus Unmanaged-APs – CVE-2016-1000213, CVE-2016-1000214, CVE-2016-1000215, CVE-2016-1000216

Initial Internal Release Date: **08/02/2016**
Initial Release to the public*:* **08/02/2016**
Update Release Date: **06/21/2017**

What is new since last advisory?

Advisory "080216" does not contain the CVE IDs for vulnerabilities reported by Tripwire. In this version "062117" the CVE IDs are now updated along with information about the fix for the vulnerabilities.

Summary

Multiple vulnerabilities were found in the Web GUI interface of Ruckus APs. These vulnerabilities were first reported by Tripwire and Ruckus acknowledges them. The vulnerabilities can be broadly classified into following two categories:

1. **CSRF exposure on Zone Flex AP:**

CVE-2016-1000213	Ruckus Wireless H500 web management interface CSRF

2. **Un-authenticated command injection and information retrieval sometimes causing denial of service attack on Zone Flex AP:**

CVE-2016-1000214	Ruckus Wireless H500 web management interface authentication bypass
CVE-2016-1000215	Ruckus Wireless H500 web management interface denial of service
CVE-2016-1000216	Ruckus Wireless H500 web management interface authenticated command injection

Workarounds

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 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.

ID 062117 FAQ

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. Following AP models with solo images are vunerable:

a) ZFxxxx (e.g. ZF7372, ZF7982)
b) Rxxx (e.g R710, R510)
c) Hxxx (e.g H500)
d) Cxxx (e.g. C110)
e) Txxx (e.g T710)
f) Exxx (e.g. E510)

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.

What releases fixes are available?

CVE ID	Status with release	Comments
CVE-2016-1000213	Not Fixed	Ruckus Wireless has plans to fix it in future releases of Zone Flex software. Since, this vulnerability is only exploitable when AP IP and web interface is accessible from external networks. Workaround is available as mentioned in previous section.
CVE-2016-1000214	Fixed in release 104.0.0.1347 for all Zone Flex APs.	For prior releases, workaround is available as mentioned in previous section.
CVE-2016-1000215	Fixed in release 104.0.0.1347 for all Zone Flex APs.	For prior releases, workaround is available as mentioned in previous section.
CVE-2016-1000216	Fixed in release 104.0.0.1347 for all Zone Flex APs.	For prior releases, workaround is available as mentioned in previous section.

How does Ruckus Wireless qualify severity of security issues?

Ruckus Wireless typically utilizes the Common Vulnerability Scoring System (CVSS) v3. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. Below are the CVSS v3 scores and vector information for respective CVEs:

CVE ID	CVSS v3 Base Score	Vector
CVE-2016-1000213	8.8 High	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVE-2016-1000214	5.3 Medium	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVE-2016-1000215	7.5 High	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2016-1000216	8.8 High	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

When will this Ruckus Wireless Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: **06/21/2017**

Ruckus Wireless released the initial security advisory to customers on: **06/21/2017**

Public posting: **06/21/2017**

ID 062117 FAQ

Revision History

ID	Change	Date
080216	Initial Publication	August 02, 2016
062117	Updated advisory with CVE IDs CVE-2016-1000213, CVE-2016-1000214, CVE-2016-1000215, CVE-2016-1000216 with latest status.	June 21, 2017

Ruckus Support can be contacted as follows:

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

DISCLAIMER