ID 101617 FAQ

Multiple Vulnerabilities discovered in 4-way handshake of WPA2 protocols

Initial Release Date: **10/16/2017**
Document Version: 1.0

What are the issues?

Ruckus has been made aware by CERT.org of certain security vulnerabilities related to the 4-way handshake of WPA and WPA2 protocols. These vulnerabilities were discovered by independent researcher Mathy Vanhoef <Mathy.Vanhoef@cs.kuleuven.be>.

Exploitation of these vulnerabilities may ultimately allow decryption of AP-client traffic, packet replay, TCP connection hijacking, and HTTP content injection. Due to these vulnerabilities, Wi-Fi Protected Access II (WPA2) handshake traffic can be manipulated to allow nonce and session key reuse, resulting in key reinstallation on a targeted wireless access point (AP) or client. For more detail about these vulnerabilities, please refer to the the Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 report. A summary of the vulnerabilities as disclosed by CERT is presented below:

CVE ID	CVE Description
CVE-2017-13077	Reinstallation of the pairwise key in the Four-way handshake
CVE-2017-13078	Reinstallation of the group key in the Four-way handshake
CVE-2017-13079	Reinstallation of the integrity group key in the Four-way handshake
CVE-2017-13080	Reinstallation of the group key in the Group Key handshake
CVE-2017-13081	Reinstallation of the integrity group key in the Group Key handshake
CVE-2017-13082	Accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it
CVE-2017-13084	Reinstallation of the STK key in the PeerKey handshake
CVE-2017-13086	Reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
CVE-2017-13087	Reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
CVE-2017-13088	Reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

What is the impact on Ruckus products?

No Ruckus products are affected unless deployed in Mesh or Point-to-Point topologies, or 802.11r is enabled.

a) **Impact of CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081:** Ruckus APs are not exposed to these vulnerabilities unless deployed in Mesh or Point-to-Point topologies.

ID 101617 FAQ

b) **Impact of CVE-2017-13082:** Ruckus APs are not exposed to this vulnerability unless 802.11r is enabled.
c) **Impact of CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088:** Ruckus APs are not exposed to these vulnerabilities.

CVE ID	Affected Product*	Comments
CVE-2017-13077	All Ruckus APs in Mesh P300 Point-to-point & Point-to-multipoint	Excludes Ruckus R300 & R310, since these models do not support Mesh
CVE-2017-13078	All Ruckus APs in Mesh P300 Point-to-point & Point-to-multipoint	Excludes Ruckus R300 & R310, since these models do not support Mesh
CVE-2017-13079	All Ruckus APs in Mesh P300 Point-to-point & Point-to-multipoint	Excludes Ruckus R300 & R310, since these models do not support Mesh
CVE-2017-13080	All Ruckus APs in Mesh P300 Point-to-point & Point-to-multipoint	Excludes Ruckus R300 & R310, since these models do not support Mesh
CVE-2017-13081	All Ruckus APs in Mesh P300 Point-to-point & Point-to-multipoint	Excludes Ruckus R300 & R310, since these models do not support Mesh
CVE-2017-13082	All Ruckus APs with 802.11r enabled	Excludes APs under SmartZone 3.2.1 and prior SmartZone releases APs managed by Ruckus Cloud are not affected

*Unless otherwise noted, these products are affected under all supported software releases. Standalone releases for access points are not impacted.

Workarounds

It is possible to completely mitigate CVE-2017-13082 by disabling 802.11r. Note that 802.11r is disabled by default in Ruckus products.

Other than disabling Mesh, there is no known workaround for CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, and CVE-2017-13081. However, because Ruckus products use CCMP for Mesh connectivity, exploitation of these vulnerabilities is made significantly difficult, as per Section 6.1 of the Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 report.

Ruckus will be releasing security patches to address all above mentioned vulnerabilities. It is recommended that customers upgrade their network(s) with these patches as soon as they become available. As they are released, these patches will be posted on Ruckus' Support site (support.ruckuswireless.com) and this security bulletin will be updated. Ruckus Cloud and Xclaim customers will be automatically updated once the security patches are available.

Ruckus also strongly recommends that customers upgrade the client devices on their network to releases which address these issues.

What releases will be available with fixes?

The following Ruckus releases will be patched with AP firmware fixes for the above mentioned vulnerabilities:

SmartZone
- 3.1.2

- 3.2.1
- 3.4.2
- 3.5.1

ZoneDirector
- 9.10.2
- 9.12.3
- 9.13.3
- 10.0.1

Unleashed
- 200.5

Ruckus Cloud

Xclaim

P300
- 100.1

Document Revision History

Version	ID	Change	Date
1.0	101617	Initial Publication	October 16, 2017

Ruckus Support can be contacted as follows:

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

DISCLAIMER