Ruckus Wireless Security Advisory ID 071715 FAQ:

Packet Injection Vulnerability on 802.11n MAC Frame Aggregation

Internal Release Date: **7-17-2015**
Release to the public***: 7-17-2015***
This Ruckus Security Advisory constitutes Ruckus Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Wireless.

What is the issue?

A potential vulnerability on 802.11n MAC Frame Aggregation feature was exposed recently. The vulnerability can potentially be used by attackers to inject frames into wireless networks by using Packet-In-Packet technique to exploit the frame aggregation mechanism introduced in 802.11n standard.

This is a flaw in the 802.11n aggregation protocol design and not Ruckus specific. Impacts all 802.11n implementations. The vulnerability has an easy workaround; enabling encryption on the wireless network will prevent this vulnerability from being exploited.

Ruckus will work with WiFi silicon vendors and provide additional checks through firmware updates if required in the future. Best defense is enabling encryption as it prevents this vulnerability from being exploited.

Do I need to check if I am vulnerable?

Packet Injection Vulnerability is a design flaw. This flaw has been identified in a technical paper published at "ACM WiSec 2015: 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks", http://www.sigsac.org/wisec/WiSec2015/. There is no need to run any specific tests to check if you are vulnerable. The probability of the success in this attack as calculated by the above-referred paper is, 1 in 4K frames. Ruckus recommends enabling of encryption on the wireless network to protect against this vulnerability.

How does Ruckus Wireless qualify severity of security issues?

Ruckus Wireless utilizes the Common Vulnerability Scoring System (CVSS) v2. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response.

This particular issue has not yet been reported and rated on the CVS System.

When will this Ruckus Wireless Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: **7-17-2015**

Ruckus Wireless released the initial security advisory to customers on: **7-17-2015**

Public posting: **7-17-2015**

Ruckus Support can be contacted as follows:

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

2 Ruckus Wireless Security Advisory ID 071715 FAQ: