Ruckus Networks - Security Advisory
ID 20180815 FAQ

Linux Kernel TCP Reassembly Algorithm Remote DOS Vulnerability

Initial Internal Release Date: **08/15/2018**
Initial Release to the public***: 08*/15/2018**
Update Release Date: **09/06/2018**

What is the issue?
A vulnerability named SegmentSmack was found in the way the Linux kernel handled specially crafted TCP packets. A remote attacker could use this flaw to trigger time and calculation expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() functions by sending specially modified packets within ongoing TCP sessions which could lead to a CPU saturation and hence a denial of service on the system. Maintaining the denial of service condition requires continuous two-way TCP sessions to a reachable open port, thus the attacks cannot be performed using spoofed IP addresses.

What action should I take?
Ruckus Networks will release a fix for this vulnerability when the upstream fix is available. It is advised to upgrade your image once it's released.

Are there any workarounds available?
Currently, no workaround is available.

What is the impact on Ruckus products?

All SmartZone products starting from ***R3.0***, as well as Cloud Wifi, are vulnerable to this vulnerability. The following table illustrates the release date for the fix.

Product	Vulnerable Release	Resolution	Patch Release Date
SmartZone	3.0, 3.1.x, 3.2.x 3.4.2.0.217(patch 3) 3.5.1 3.6.0/3.6.1 5.0	Apply fix when available Apply fix when available Apply fix when available Upgrade to 3.6.2 Patch 1 Upgrade to 5.1	Dec 2018 Dec 2018 Dec 2018 Dec 2018 Nov 2018
Cloud Wifi	18.02.x	N/A	TBD

ID 20180815 FAQ

How does Ruckus 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. In cases where CVSS v3 scores are not available, CVSS v2 score are provided. Below are the CVSS scores and vector information for respective CVEs:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2018-5390	7.5 (High)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

When will this Ruckus Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: 08/15/2018
Ruckus Wireless released the initial security advisory to customers on: 08/15/2018
Public posting: 08/15/2018

Revision History

Version	ID	Change	Date
1.0	20180815	Initial Release	Aug 15, 2018
1.1	20180815	Updated the fix date	Aug 21, 2018
1.2	20180815	Updated the fix details	Sept 6, 2018

Ruckus Support can be contacted as follows:

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

DISCLAIMER