Ruckus Networks - Security Advisory

ID 20190815 FAQ

TCP SACK PANIC – Kernel Vulnerability – CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479

Initial Internal Release Date: **08/15/2019**
Initial Release to the public**: 08/15/2019**
Update Release Date: **N/A**

What is the issue?
Three flaws were found in the Linux kernel's handling of TCP networking. The most severe vulnerability could allow a remote attacker to trigger a kernel panic in systems running the affected software and, as a result, impact the system's availability.

The issues have been assigned multiple CVEs: CVE-2019-11477, CVE-2019-11478 and CVE-2019-11479. They are all considered as HIGH severity. The first two are related to the Selective Acknowledgement (SACK) packets combined with Maximum Segment Size (MSS), the third solely with the Maximum Segment Size (MSS). A remote attacker can use these flaws to cause a denial of service (DoS) by sending a sequence of crafted packets on a TCP connection.

What action should I take?
Ruckus Networks is releasing the fix for these vulnerabilities via software update. Since these are serious issues, all customers are strongly encouraged to apply the fix once available.

Are there any workarounds available?
None

What is the impact on Ruckus products?

The following table describes the vulnerable products, software version and the recommended action:

Product	Vulnerable Release	Resolution	Patch Release Date
SmartZone, SZ AP	3.0, 3.1.x, 3.2.x, 3.4.x 3.5.x, 3.6.x 5.0/5.1	See (1) below Upgrade to 3.6.2 Patch 2 Upgrade to 5.1.3	See (1) below Oct 2019 Feb 2020
ZD	9.10.x 9.12.x 9.13.x, 10.0.x 10.1.x 10.2.x 10.3.x	Upgrade to 9.10.2 MR2 Refresh 7 Upgrade to 9.12.3 MR3 Refresh 8 Upgrade to 10.0.1 MR1 Refresh 6 Upgrade to 10.1.2 MR2 Refresh 3 Upgrade to 10.2.1 MR1 Refresh Upgrade to 10.3.1 MR1 Refresh	Dec 2019 Dec 2019 Oct 2019 Sept 2019 Nov 2019 Oct 2019
Unleashed	200.6, 200.7	Upgrade to 200.7.10.102 MR Re-fresh	Nov 2019
vSPoT	All versions	Under investigation	TBD
SCI	5.2.1	Upgrade to 5.3	Aug 2019
IoT Controller	GA-1.0 to GA-1.4	Upgrade to GA-1.5	Dec 2019
ICX	All versions	Under investigation	TBD

(1): Please contact Customer Support https://support.ruckuswireless.com/contact-us

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. Below are the CVSS scores and vector information:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2019-11477	7.5 (HIGH)	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2019-11478	7.5 (HIGH)	(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2019-11479	7.5 (HIGH)	(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: 08/15/2019
Ruckus Wireless released the initial security advisory to customers on: 08/15/2019
Public posting: 08/15/2019

Revision History

Version	ID	Change	Date
1.0	20190815	Initial Release	Aug 15th, 2019

Ruckus Support can be contacted as follows:

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

DISCLAIMER

THIS RUCKUS NETWORKS SECURITY ADVISORY INCLUDING THE INFORMATION IT CONTAINS AND THE PROGRAMS MADE AVAILABLE THROUGH THE LINKS THAT IT INCLUDES, IS PROVIDED TO YOU ON AN "AS IS" BASIS. RUCKUS NETWORKS (AN ARRIS COMPANY) AND ITS SUPPLIERS DO NOT WARRANT THAT SUCH INFORMATION OR THE FUNCTIONS CONTAINED IN SUCH PROGRAMS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAMS WILL BE UNINTERRUPTED OR ERROR-FREE. THE INFORMATION AND PROGRAMS ARE PROVIDED TO YOU WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT WILL RUCKUS NETWORKS (AN ARRIS COMPANY), ITS SUPPLIERS, OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE INFORMATION OR PROGRAMS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOST DATA, THAT MAY ARISE OUT OF YOUR USE OF OR FAILURE TO USE THE INFORMATION OR PROGRAMS, EVEN IF RUCKUS NETWORKS (AN ARRIS COMPANY) OR SUCH OTHER ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING SHALL NOT BE DEEMED TO PRECLUDE ANY LIABILITY, WHICH UNDER APPLICABLE PRODUCTS LIABILITY LAW, CANNOT BE PRECLUDED BY CONTRACT.