Ruckus Networks - Security Advisory

ID 20180906 FAQ

Intel Speculative Execution Vulnerabilities – CVE-2018-3615 CVE-2018-3620 & CVE-2018-3646

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

Summary

Security researchers have identified a speculative execution side-channel method called L1 Terminal Fault (L1TF) affecting select Intel processors. Intel has published a security advisory for these vulnerabilities. The same can be referred here: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html

What are the issues?

These vulnerabilities are assigned the CVE IDs and details of the same are explained as below:

CVE ID	CVE Description
CVE-2018-3615	Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.
CVE-2018-3620	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.
CVE-2018-3646	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.

ID 20180906 FAQ

What is the impact on Ruckus products?
No Ruckus products are impacted.

What is the impact on ICX family of switches that are part of Ruckus now?
No Ruckus ICX, Brocade FastIron and TurboIron switches are impacted.

Why are Ruckus products not impacted?
Ruckus Networks products are based on a number of different CPU architectures (ARM, Intel, PPC etc) some of which are affected by these vulnerabilities.
All Ruckus products only run software that are integral to the system and do not allow installation of arbitrary software from unauthorized users. For an attacker to exploit this vulnerability, one has to gain access to the system using another vulnerability. We recommend that customers always install any patches released as per our security advisories. Please refer to some caveats below.

Caveats:
Ruckus has been closely working with our cloud providers supporting products such as Ruckus Cloud, Cloudpath. They are either in the process of applying, or have already applied, mitigation patches to their virtualization environments.

Virtual appliance products such as virtual SmartZone controller, Virtual SPoT, SCI and Cloudpath on-prem software run on virtualization platform hypervisors. It is advised that customers contact the host OS / hypervisor vendors to patch the systems to address any vulnerabilities that might allow an attacker to gain access to the host OS memory modules and there-by access into the guest OS (like our virtual appliances) memory systems and cause undesired results.

What action do I take?
No immediate action is required.
Ruckus is actively investigating available kernel patches, CPU microcode updates, and other mitigations and may deploy these in future software releases.

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-2018-3615	6.4 (Medium)	(AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N)
CVE-2018-3620	5.6 (Medium)	(AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)
CVE-2018-3646	5.6 (Medium)	(AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

Revision History

Version	ID	Change	Date
1.0	20180906	Initial Release	September 06, 2018

Ruckus Support can be contacted as follows:

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

DISCLAIMER