Zombieload, RIDL and Fallout vulnerabilities CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2018-11091

Initial Internal Release Date: **05/28/2019**
Initial Release to the public*: 05/28/2019*
Update Release Date: **05/28/2019**

This "Ruckus Networks Security Advisory" constitutes Ruckus Networks (an ARRIS company) Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Networks (an ARRIS company).

Summary

This is in response to Intel's recent micro-architectural data sampling advisory impacting many Intel products. Intel has enumerated the platforms and the firmware versions impacted by these security vulnerabilities. Intel's complete security advisory can be found here: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.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-2018-12126	Micro-architectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2018-12127	Micro-architectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2018-12130	Micro-architectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2018-11091	Micro-architectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

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

What is the impact on Ruckus ICX, Brocade FastIron and TurboIron 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 (including Intel) 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 these side-channel vulnerabilities, 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 security patches and other mitigations and would deploy these in future releases. Ruckus is doing the due diligence to test the impact of these patches on our quality, performance and resiliency.

How does Ruckus qualify severity of security issues?
Ruckus Networks 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-2018-12126	6.5 (Medium)	(AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)
CVE-2018-12127	6.5 (Medium)	(AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)
CVE-2018-12130	6.5 (Medium)	(AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)
CVE-2018-11091	3.8 (Low)	(AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N)

Revision History

Version	ID	Change	Date
1.0	20190528	Initial Release	May 28, 2019

Ruckus Support can be contacted as follows:

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

DISCLAIMER