Ruckus Networks - Security Advisory
ID 20180618 FAQ

SPECTRE NG Vulnerabilities – CVE-2018-3639, CVE-2018-3640

Initial Internal Release Date: **06/18/2018**
Initial Release to the public**: 06/18/2018**
Update Release Date: **06/18/2018**

Summary

Google Project Zero team and other researchers have reported Spectre and Meltdown, CPU architecture level vulnerabilities earlier in January 2018. In May 2018, researchers from Intel and Google have reported some more similar vulnerabilities of spectre family which are termed as variant 4 (Spectre Next Generation – NG) associated with CVE-2018-3639 and variant 3a, associated with CVE-2018-3640. Both variants use cache-timing attacks that may allow an attacker to obtain access to sensitive information on affected systems.

What is the issue?

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

CVE ID	CVE Description
CVE-2018-3639	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
CVE-2018-3640	Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis, aka Rogue System Register Read (RSRE), Variant 3a.

What is the impact on Ruckus products?

None of the Ruckus Network Products are found to be vulnerable against these vulnerabilities till the time of publishing this security advisory. However, detailed analysis and investigation is under process and this security bulletin will be updated with latest information as soon as the investigation is complete.

Ruckus Networks products are based on many different CPU architectures (ARM, Intel, PPC etc) some of which are affected by these vulnerabilities. All Ruckus Network 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 vulnerabilities, (s)he has to gain access to

the underlying OS system which is heavily protected as we do not allow users direct to access OS and control the user system interaction via GUI or CLI.

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 should I take?
If deployment consist of any Ruckus Network Products deployed as Virtual machine then even the Ruckus Products are not directly vulnerable, but underlying hosting OS / hypervisor may be vulnerable. Hence, it is advised that in above mentioned environment(s) customer(s) should contact the vendors of the Host OS / Hypervisor for the update of the latest patches which contain the fix / workaround for these vulnerabilities.

Ruckus is actively investigating available kernel patches, CPU microcode updates, and other mitigations and may deploy these in future software releases. This security advisory with updates will be published soon as the investigation is complete.

We recommend that customers always install any patches released as per our security advisories. Please refer to some caveats below.

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

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 Base Score	Vector
CVE-2018-3639	4.3 (Medium)	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N
CVE-2018-3640	4.3 (Medium)	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

When will this Ruckus Security Advisory be publicly posted?
Ruckus Wireless released the initial security advisory to Ruckus field teams on: 06/18/2018
Ruckus Wireless released the initial security advisory to customers on: 06/18/2018
Public posting: 06/18/2018

Revision History

Version	ID	Change	Date
1.0	20180618	Initial Release	June 18, 2018

Ruckus Support can be contacted as follows:

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

DISCLAIMER