

ID 20180105 FAQ**Spectre and Meltdown Vulnerabilities – CVE-2017-5753 CVE-2017-5715
& CVE-2017-5754**Initial Internal Release Date: **01/05/2018**Initial Release to the public: **01/05/2018**Update Release Date: **01/10/2018**

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

Google Project Zero team and other researchers have reported Spectre and Meltdown, CPU architecture level vulnerabilities. Exploitation of these vulnerabilities could potentially lead to privilege level information disclosure. For more detail about these vulnerabilities, please refer here:

<https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.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-2017-5753 | Systems with processors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information via a side-channel analysis. |
| CVE-2017-5715 | Systems with processors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information via a side-channel analysis. |
| CVE-2017-5754 | Systems with processors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information via a side-channel analysis of data cache. |

ID 20180105 FAQ**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?

All Ruckus ICX, Brocade FastIron and TurboIron switches are not 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 thereby 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. While there are some mitigation techniques available that are known to reduce system performance significantly, Ruckus is doing the due diligence to test the impact of such patches on our quality, performance and resiliency.

ID 20180105 FAQ**Revision History**

| Version | ID | Change | Date |
|----------------|-----------|--------------------------------|------------------|
| 1.0 | 20180105 | Initial Release | January 05, 2018 |
| 1.1 | 20180105 | Updated FAQ for wired products | January 10, 2018 |

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.

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).

© Copyright 2018 Ruckus Networks, an Arris company. All Rights Reserved