TECHNICAL SUPPORT

SECURITY ADVISORY

Meltdown and Spectre - Processor (CPU) Speculative Execution Side-Channel Attack Vulnerabilities

BULLETIN ID:	00011303
PUBLISHED:	2018-01-05
REVISION:	1
TYPE:	Bulletin

Background:

Ribbon is aware of recently disclosed research regarding side-channel attacks using speculative execution performance optimization in most modern processors (CPUs). These side channel attacks, recently branded as “Meltdown” and “Spectre”, provide a method for an attacker to observe contents of privileged memory, bypassing any expected privilege levels and security checks.

Analysis:

Researchers have identified three attack variants that could be used to exploit vulnerable processors:

- Variant 1: Bounds check bypass (CVE-2017-5753)
- Variant 2: Branch target injection (CVE-2017-5715)
- Variant 3: Rogue data cache load (CVE-2017-5754)

The Spectre attack refers to attack variant one and two, while Meltdown refers to variant three.

Ribbon is currently assessing the impacts of these vulnerability exploits across its product portfolio and actively following patch updates from OS vendors (e.g. RedHat, etc.) as they become available. Ribbon will also be performing capacity benchmark testing on any code or

patch updates given industry statements around potential degradations and this information will be communicated as required.

In order to exploit any of these vulnerabilities, an attacker must be able to execute crafted code on an affected product. Ribbon products are closed systems, which do not allow installation of any unauthorized software. Most Ribbon products and solutions are also deployed in private/trusted and managed networks, with other security access controls and defense-in-depth measures to help mitigate any risks of exploit.

For customers with Ribbon products running in their own virtualization environment (versus a Ribbon closed/hosted virtualization environment), Ribbon encourages customers to assess the risks and impacts as necessary since these exploits may also allow a Virtual Machine (VM) instance to glean memory data from the host system (e.g. hypervisor) and other VM instances (tenants/guests).

Recommendations:

Please refer to the following Ribbon external link/article for further updates on this bulletin as they become available:

https://support.sonus.net/display/PORTAL/Meltdown+and+Spectre%3A+Processor+%28CPU%29+Speculative+Execution+Side-Channel+Attack+Vulnerabilities

Required Actions:

There are no required actions for this bulletin.

Additional Information:

Further information is also available on the following sites:

https://meltdownattack.com/

https://www.us-cert.gov/ncas/alerts/TA18-004A

https://access.redhat.com/security/vulnerabilities/speculativeexecution

https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

Attachments:

There are no attachments for this bulletin.

Products and Releases:

The information in this bulletin is intended to be used with the following solutions/products and associated releases:

SOLUTION	SOLUTION RELEASE(S)	PRODUCT	RELEASE(S)
All Solutions	Applicable to all Releases	All Products	Applicable to all Releases

To view the most recent version of this bulletin, access technical documentation, search the knowledge base, or contact Technical Support, please log in to Services | Customer Support Portal at: http://cust.genband.com.

DOCUMENT REFERENCE:
PATCH ID:
FIXED RELEASE:

You may sign up to receive automatic email alerts when new bulletins are published or existing bulletins are updated from the Document Center, under the "Sign up for notifications" link.