Spectre & Meltdown FAQ

Author: John R. Naylor, Technology Strategist, CTO Office, Ross Video
Date: January 18, 2018

What are Spectre and Meltdown?

Both are exploits that target vulnerabilities in processors from Intel, ARM and AMD. In some cases, the vulnerabilities date back to 1995. In other words, pretty much every modern processor in use today is affected.

The damage they can do is limited to obtaining copies of private information. They cannot themselves take over your machine or run malware. However, the information obtained by them may enable follow-on attacks that can.

Which Computers are at Risk?

Machines that are shared with strangers, such as cloud-hosted ones, are the most vulnerable to these attacks. The risk envelope is much smaller for machines that are protected by good physical and network security. If an attacker cannot run their code on a machine, they cannot exploit these vulnerabilities.

What Ross Products are Affected?

Like all other companies in the Broadcast industry, Ross makes extensive use of processors from Intel and ARM across our product range. We have classified our product range by vulnerability to Spectre and Meltdown below:

Product Type	Examples	Vulnerability	What Action Should I Take?
Cloud-based products and Software as a Service (SaaS)	Inception Cloud	Because these products are hosted on machines that are shared with other users the vulnerability of products in this class is generally Medium. However, Ross has ensured that the necessary patches have been installed by our cloud service providers to eliminate these vulnerabilities. So, the operational vulnerability is **None**.	None. We have already applied the necessary fixes via our cloud service providers.

Server-based Turnkey Products	XPression OverDrive Inception Abekas	If you have provided good physical security for the server room or rack room in which you host these products, and can limit both physical and network access to them to trusted people the vulnerability of products in this class is **Low** to **None**.	Products in this class require both Operating System and BIOS patches which we expect to be available by the start of February 2018.
		If access to products in this class is uncontrolled and people outside your trusted group can access these products (e.g. in a rental scenario) their vulnerability is **Medium**.	Improve your physical and operational security practices so that physical and network access is limited to those you know and trust. For systems that do not run anti-virus protection for performance reasons, consider taking them offline and perform vulnerability scans
Embedded Products	Carbonite Acuity openGear Caprica	Products in this class do not support general purpose use or the installation of 3rd party applications. Their vulnerability is therefore **None.**	No action necessary.

What Fixes are Available for Ross Products?

At present, there is not a comprehensive set of fixes that can be applied to all Ross Products. This is because patches are required at the BIOS, as well as the Operating System level. We are working with our suppliers to obtain the necessary patches as a matter of urgency.

Until a fix is both available and qualified by Ross Video, we strongly advise our customers to minimize their risk by applying the following best practices:

- Avoid running unnecessary software on turnkey systems, especially web browsers.
- Ensure your virus definitions and scanner engines are up to date.
- If you're running products without anti-virus protection for performance reasons, consider taking them offline and performing a vulnerability scan.
- Limit physical and network access to your server-based products to people you know and trust.
- If using rental equipment that you obtained later than June 2017, ensure that it was in a factory default state when you took delivery. Consider performing a virus scan to reduce the chances that malware that can exploit these vulnerabilities is present.

What is the Performance Impact of the Fixes?

The fixes for Spectre and Meltdown remove a performance optimization, which is the source of the system vulnerability. That is why the fixes can affect system performance. However, the degree of degradation is *highly* dependent on the way the system is used. Ross is assessing the impact of the fixes on each affected product, which is a time-consuming process. Since starting tests at the beginning of the New Year we have yet to discover a material performance penalty. Please appreciate that this is preliminary information which is subject to change.

What do the Severity Ratings Mean?

These are based on the National Vulnerability Database (NVD) ratings, version 3.0 for these vulnerabilities. The database is operated by the USA's National Institute for Standards and Technology, NIST. The NVD's ratings for both Spectre and Meltdown is **Medium**. However, many Ross products are not susceptible to attack, or have already been remedied, which is why they appear at lower ratings in the table above.

Where can I get More Information?

Spectre and Meltdown map to three specific entries in NIST's National Vulnerability Database. Here are the links to the technical details:

CVE-2017-5715
CVE-2017-5753
CVE-2017-5754

What Support is Available from Ross Video?

We are actively working to address the Spectre/Meltdown situation on behalf of our customers. Currently, we are testing patches for impacted products. Our technical support team is committed to answering any questions you may have about how to minimize your current risk and how to run vulnerability scans, along with any other questions or concerns you may have.

At Ross Video, we prize customer success above all else. Once we have completed testing the patches, we will make them available to all customers at no charge. As well, we will provide assistance with patch application at no charge.

How do I Contact Ross Video?

Ross Technical Support is staffed by a team of experienced specialists ready to assist you with any question or technical issue.

Phone:

- Our North America center located in Ottawa, Ontario, Canada and is open Monday to Friday 8:30 a.m. to 6:00 p.m. EST, with 24/7/365 on-call service after hours.
    - **Our telephone number is: +1-613-652-4886 (Toll free within North America +1 844-652-0645)**

- Our EMEA center is located in Buckinghamshire, England, United Kingdom and is open Monday to Friday 8:30 a.m. to 5:00 p.m. GMT. After hours support is provided by our North America location.
    - **Our telephone number is: 01753 656 101 (Toll free International +800 1005 0100)**

- Our Australia/Sydney office is located in Alexandria, NSW. Our local support number is 1300 007 677. If the local support specialist is not available, your call will be transferred automatically to our North America center.

Emergency after-hours support:

+1-613-349-0006 (Toll free within North America +1 844-652-0645, International +800 1005 0100)

Email: techsupport@rossvideo.com

Website:

Support requests can be open at the following link www.rossvideo.com/support/tech-support.html