SPACELABS
HEALTHCARE

30 March 2018

Meltdown and Spectre Vulnerabilities

Meltdown and Spectre are the common names assigned to a set of cyber security vulnerabilities that have been discovered in a wide variety of processing chips architected or produced by a number of vendors, including Intel, ARM, and AMD.

These vulnerabilities are forcing a redesign of the firmware and operating system software in Windows, Mac, and Linux on machines running affected processors.

Meltdown and Spectre are members of a class of vulnerabilities referred to as "speculative execution side-channel attacks". The impact of these vulnerabilities is that an attacker could obtain content from memory regions that should not be accessible. At present, these are largely theoretical vulnerabilities (shown in proof of concept, but with no known attacks). A pre-requisite to exploitation of these vulnerabilities is that an attacker must be able to execute code on a system with an affected processor without applied mitigations.

Meltdown was assigned CVE-2017-5754 by MITRE, and is known to affect processors from Intel and ARM. Spectre was assigned CVE-2017-5753 and CVE-2017-5715, and is claimed to affect most processor vendors.

Spacelabs has determined that the underlying chip architecture for some of our patient monitoring products is potentially vulnerable to this exploit; however, the manner in which the products are used reduces the risk of the vulnerability.

Vendors of processors, firmware, and operating systems are working to release updates that are intended to mitigate these vulnerabilities. As appropriate, Spacelabs will implement updates into future versions of our products.

Spacelabs is committed to ensuring the safety, security and integrity of its products. It is a regulatory requirement that any product changes (including security updates and patches to the operating system) must be verified and validated via an accepted Quality Assurance process, as these changes can potentially affect the stability, compatibility and/or performance of products. It is Spacelabs policy that any changes to Spacelabs hardware products (including software patches or updates) may only be performed by certified field service staff.

Microsoft has released operating system updates for these vulnerabilities (see Microsoft resources and KB4090007). Health delivery organizations that host and use Spacelabs software solutions are encouraged to analyze this information closely, and as appropriate keep their infrastructure patched and up to date. Spacelabs has ongoing test protocols to ensure that its software products are not operationally impacted by host infrastructure patching.

If you have additional concerns about these vulnerabilities, Spacelabs recommends you contact your Spacelabs Technical Support Representative via for further information. Technical support can be reached at 800-522-7025, option 2; or via email at techsupport@spacelabs.com

Additional Resources

- The United States Department of Homeland Security (DHS) Computer Emergency Response Team (CERT) for Industrial Control Systems (ICS) has posted the following bulletin: Meltdown and Spectre Vulnerabilities
- There are a number of good technical papers posted to describe these attacks in detail, including: https://meltdownattack.com/