Meltdown and Spectre Threat

Meltdown: CVE-2017-5754; Spectre: CVE-2017-5753 and CVE-2017-5715

Purpose

This technical note provides information about the recent Meltdown and Spectre threat which exploits critical vulnerabilities in nearly all processors, including intel, AMD, and ARM since 1995.

Products

All Server Technology Power Distribution Units (PDUs) and the Sentry Power Manager (SPM) enterprise software product.

Vulnerability Summary

The hardware vulnerabilities – nicknamed “Meltdown” and “Spectre” – for the Intel, AMD, and ARM processors allow programs to steal data that is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include encryption keys, passwords stored in a password manager or browser, emails, instant messages, business-critical documents, and more.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the infrastructure of the cloud provider, it might be possible to steal data from other customers.

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system. Most computer processors are vulnerable to this attack and can potentially be exploited to steal sensitive information and data. This applies to personal computers, servers, and cloud infrastructure.

Spectre breaks the isolation between different applications, allowing an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of these best practices actually increase the attack surface and may make applications more susceptible to Spectre. Spectre is harder to exploit than Meltdown, but it is also harder to mitigate.

Server Technology PDUs

Note: Server Technology PDUs are **NOT** vulnerable to Meltdown and Specter.

Determining Factors:

Server Technology PDUs use processors that are not affected, and run firmware that is a closed platform.

Unaffected Processors:

Server Technology PDUs use an ARM processor core. Arm has published a definitive list of which Arm-designed processors cores are potentially susceptible:

www.arm.com/security-update

Server Technology PDUs use Digi International NET+ARM processors:

- PDUs with a NIM2 NIC (which run v8.x firmware) use a Digi NS9215 chip with an **ARM926EJ-S** (ARM9) processor core.
- PDUs with a NIM1/ME NIC (which run v7.1 and earlier firmware) use a Digi NS7520 chip with an **ARM7TDMI** (ARM7) processor core.

These ARM processor cores are NOT in the affected list.

Closed Platform:

Server Technology PDU firmware runs a non-open environment where processes are strictly controlled. User applications are not supported, and hence not exploitable towards these vulnerabilities, which require running a malicious application.

Conclusion:

Server Technology PDUs are NOT affected by the threats.

Server Technology's Sentry Power Manager (SPM)

VMware:

For VMware systems, it is recommended to patch the server that hosts the VMware application.

https://vinfrastructure.it/2018/01/meltdown-spectre-vmware-patches/

Appliances:

Appliance SPM systems use Intel processors that may be susceptible to Meltdown and Spectre. A Meltdown patch is available for SPM version 6.2.2, as well as a partial patch for Spectre. For assistance, contact Server Technology Technical Support. (See contact information at the end of this document.)

Server Technology will release additional security patches as they are officially released by Canonical, the makers of Ubuntu.

https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown

https://newsroom.intel.com/news/intel-responds-to-security-research-findings/

Closed System:

Meltdown and Spectre are exploited by running a malicious application. The risk for SPM is smaller because normal usage of SPM does not give users access to run applications on the SPM server or to access the root operating system. Even so, it is strongly recommended to apply the security patches as they become available and to keep your SPM version up-to-date.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.
1040 Sandhill Drive   Tel: 1-800-835-1515   Web: www.servertech.com
Reno, Nevada 89521 USA   Fax: 775-284-2065   Email: support@servertech.com

Server Technology, the Globe logo, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.