Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

Spectre and Meltdown Security Vulnerabilities

Date: 2019-03-08 **DocumentID: SEC-03-180926**

Background

Two security vulnerabilities known as **Spectre** and **Meltdown** have received significant news coverage and prompted responses from processor companies, operating system companies, and cloud providers.

What Spectre and Meltdown Do

Modern processors perform “speculative execution,” which is essentially attempting to execute instructions before assuring that those instructions need to be executed. For example, the processors will guess at which way a branch might be taken and execute instructions on the basis of that guess. If the guess is correct, the processor completes work without having to wait to see if the branch was taken or not. If the guess is wrong, results are discarded and the processor resumes executing the correct side of the branch.

While this speculative execution does not alter program behavior, the Spectre and Meltdown vulnerabilities make it possible for one process to infer properties of data belonging to another process. This enables potential information leakage that can be used maliciously to steal information (e.g., passwords stored by a Web browser) or leveraged by other security flaws to increase their impact.

What Processors and Systems Are Affected

Affected processors include most Intel and some AMD and ARM chips. Affected systems include Windows, Linux, Android, Chrome, iOS, and MacOS (including laptops, embedded devices, servers, clients, mobile phones, etc.). Details regarding both of these vulnerabilities and the affected vendors’ respective impacted products and responses may be found here. Researchers have authored papers on Spectre (CVE2017-5715 and CVE-2017-5053) and Meltdown (CVE-2017-5754) attacks and Proof of Concept exploit code is publicly available in languages including C++, JavaScript, and C.

Trademarks are the property of their respective owners.
© 2019 Vyaire. Vyaire, the Vyaire logo and all other trademarks or registered trademarks are property of Vyaire Medical, Inc., or one of its affiliates.

Response

How Affected Suppliers and Medical Device Manufacturers Are Responding

Many vendors – including Microsoft, Apple, Amazon, Google, Linux kernel developers, VMware and Citrix – have already released patches; others are continuing to roll out such patches. Intel, AMD and ARM all have published public advisories and detailed whitepapers regarding products affected and mitigation plans.

How Vyaire Is Impacted

Microsoft has updated its Azure cloud computing platform to protect against Meltdown, forcing a reboot of some of Vyaire's Azure-based virtual machines. Guarding against Spectre will still need operating system and application-level changes. Microsoft has incorporated corrective operating system patches into its more recent updates, some of which already have been applied to Vyaire internal systems, with more to follow as they become available.

Affected Products

Vyaire's medical devices potentially affected include all Windows-based Respiratory products and possibly some Ventilator products. RKP application servers also will need to be patched as subsequent updates become available from Microsoft.

Next Steps

- As further O.S. updates/patches are made available by their respective vendors and tested, Vyaire IT will continue to deploy them with urgency to all endpoints, servers and network infrastructure components.
- Product teams are advised to identify all Vyaire systems using any controller boards that leverage the affected CPUs and develop action plans – including remediation actions such as O.S. and/or firmware updates and potential customer action requirements – to secure those systems.
- Vyaire IT will provide advisory support and assistance as needed to the Product Engineering teams in order to ensure we stay on top of this evolving situation.
- Monitor NH-ISAC, ICS-CERT, and other resources

Trademarks are the property of their respective owners.
© 2019 Vyaire. Vyaire, the Vyaire logo and all other trademarks or registered trademarks are property of Vyaire Medical, Inc., or one of its affiliates.
VYR-GBL-1900002

Security Bulletin

IMPORTANT INFORMATION – PLEASE READ AND KEEP

Generic controls

- Ensure that the patches made available by Microsoft have been applied to the operating system of your computers:
  - Microsoft Advisory: Apply patches for ADV180002, updated January 2018.
  - Vyaire tests and approves applicable patches that Microsoft identifies as critical or security related. Vyaire is prioritizing validation efforts for the Microsoft patches released for Meltdown and Spectre vulnerabilities.
- Ensure that applicable firmware updates made available by your device manufacturer are applied.
- Ensure your data has been backed up and stored according to your individual process and that your disaster recovery procedures are in place.
- Update your anti-virus and malware protection, where available.

For additional technical details and indicators associated with this vulnerability, review Vulnerability Note VU#584653

For product or site-specific concerns, contact your Vyaire service representative.

For more information on Vyaire's proactive approach to product security and vulnerability management, contact us under: http://www.vyaire.com/productsecurity

Trademarks are the property of their respective owners.
© 2019 Vyaire. Vyaire, the Vyaire logo and all other trademarks or registered trademarks are property of Vyaire Medical, Inc., or one of its affiliates.