Vulnerability advisory

Meltdown Sceptre Security Advisory

Date:	Jan 16, 2018
Subject:	Meltdown Spectre Vulnerabilities
Product:	Eaton Products using Intel, AMD, ARM processors
Severity rating:	Medium

Summary

Security researchers have recently uncovered security issues known as ‘Meltdown’ and ‘Spectre’ affecting almost all modern computer processors. These issues take advantage of modern CPU performance feature called speculative execution.

The Meltdown and Spectre exploitation techniques leverage speculative execution to gain privileged access to memory (including kernel) and allow programs to steal data currently being processed by the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre vulnerabilities to bypass these controls and get hold of secrets of other running programs stored in the memory. This might include passwords stored in a password manager or browser, private keys, session-ids etc.

In-depth technical analysis

Please refer to the CERT Vulnerability Note (VU#584653) for detailed analysis on these attacks http://www.kb.cert.org/vuls/id/584653

Potential Impact on Eaton Products

Eaton Product Cybersecurity CoE has reviewed these issues and has determined that likelihood of an attacker successfully exploiting these vulnerabilities on Eaton products is low and therefore assigned a severity rating of **Medium** (same severity level that has been assigned by DHS-ICS CERT).

Eaton continues to evaluate the potential exposure of its products to these vulnerabilities. Any additional information will be published on Eaton Cybersecurity website www.eaton.com/cybersecurity

References

Spectre and meltdown attack
https://spectreattack.com/

CERT
http://www.kb.cert.org/vuls/id/584653
Intel - https://security-center.intel.com/advisories.aspx

ARM -
https://developer.arm.com/support/security-update

AMD -
https://www.amd.com/en/corporate/speculative-execution

Additional information

For additional information or a list of vulnerabilities that have been reported on Eaton products and how to address them, please visit our Cybersecurity website www.eaton.com/cybersecurity or contact us at CybersecurityCOE@eaton.com.

Powering Business Worldwide

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in XXX
Publication No. BRXXXXXXXXE / XXX
Jan 2018

Follow us on social media to get the latest product and support information.