SSB-068644: General Customer Information for Speculative Side-Channel Vulnerabilities in Microprocessors

Publication Date 2018-01-11
Last Update 2018-08-17
Current Version V1.4

SUMMARY

Security researchers published information on vulnerabilities known as Spectre, Meltdown, Spectre-NG, Lazy FP State Restore, Spectre V1.1, and L1 Terminal Fault/Foreshadow. These vulnerabilities affect many modern processors from different vendors to a varying degree.

Siemens is analyzing the impact of these vulnerabilities and of the mitigations released on its own products**.** If Siemens products are found to be affected, additional product-specific update information will be distributed either via the Siemens ProductCERT website [1] or through Siemens' customer service organizations if applicable.

Vendors of affected processors, operating systems and other software, e.g. Internet Browsers, are assessing the vulnerabilities and are releasing updates which help to mitigate these vulnerabilities.

Several Siemens products can be installed on systems that include affected processors and use operating systems which provide mitigating patches. This document provides:

- General guidance for customers who are responsible for managing systems that run Siemens products;
- Information on the vulnerabilities;
- General recommendations for applying related operating system patches, microcode updates and 3rd party software updates.

VULNERABILITY DETAILS

Spectre, Meltdown, Spectre-NG, Lazy FP State Restore, Spectre V1.1, and L1 Terminal Fault/Foreshadow are vulnerabilities from 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.

A pre-requisite to exploitation of these vulnerabilities is that an attacker must be able to execute untrusted code on a system with an affected processor without applied mitigations.

The class of vulnerabilities referred to as "speculative execution side-channel attacks" comprises the following disclosed vulnerabilities:

Spectre (Vulnerability disclosures from 2018-01-04):

- Spectre Variant 1 was assigned CVE-2017-5753 and is claimed to affect most processor vendors
- Spectre Variant 2 was assigned CVE-2017-5715 and is claimed to affect most processor vendors.

Meltdown (Vulnerability disclosures from 2018-01-04):

- Meltdown was assigned CVE-2017-5754 and is known to affect processors from ARM, IBM, and Intel.

Spectre-NG (Vulnerability disclosures from 2018-05-21):

- Spectre Variant 3a was assigned CVE-2018-3640 and is known to affect processors from ARM and Intel.
- Spectre Variant 4 was assigned CVE-2018-3639 and is claimed to affect most processor vendors.

Lazy FP State Restore (Vulnerability disclosure from 2018-06-13):

- Lazy FP State Restore was assigned CVE-2018-3665 and is known to affect processors from Intel.

Spectre V1.1 (Vulnerability disclosure from 2018-07-10):

- Spectre Variant 1.1 was assigned CVE-2018-3693 and is claimed to affect most processor vendors.

L1 Terminal Fault / Foreshadow (Vulnerability disclosure from 2018-08-14)

- L1 Terminal Fault: SGX was assigned CVE-2018-3615 and is known to affect most processors from Intel.
- L1 Terminal Fault: OS/SSM was assigned CVE-2018-3620 and is known to affect most processors from Intel.
- L1 Terminal Fault: VMM was assigned CVE-2018-3646 and is known to affect most processors from Intel.

Detailed information on these vulnerabilities has been published by the researchers [2, 3, 4, 5, 6, 7], as well as by vendors of operating systems and processors, such as Microsoft [13, 14, 15, 16, 17, 18] or Intel [8, 9, 10, 11, 12].

RECOMMENDATIONS

Vendors of processors, operating systems, and other applications are releasing updates that help to mitigate these vulnerabilities. Siemens is analyzing the impact of these vulnerabilities on its own products. If Siemens products are found to be affected, additional product-specific update information will be distributed either via the Siemens ProductCERT website [1] or through Siemens' customer service organizations if applicable.

Updates for operating systems, processor firmware, and other systems can help to mitigate these vulnerabilities. Siemens is testing the compatibility of the patches released for supported operating systems for several products.

Siemens is aware that some updates can result in compatibility, performance or stability issues on certain products and operating systems. Operating system vendors, such as Microsoft, are still working to address these compatibility issues with their updates. Siemens will therefore continue to evaluate the applicability of those updates.

Siemens recommends consulting the product support documentation via the usual information channels, or to contact Siemens' customer service for information on compatibility before applying the updates.

As a general guidance, Siemens recommends that customers evaluate the following:

- Determine if vendors of the processors, operating systems and other software used on the computer systems have released mitigations for these vulnerabilities.

- As a pre-requisite for an attack, an attacker must be able to run untrusted code on affected systems. Therefore, Siemens recommends determining if it is possible that untrusted code can be run on these systems, or if existing measures implemented by the operator reduce the likelihood of untrusted code being run.

- Applying a Defense-in-Depth concept [20] can help to reduce the probability that untrusted code is run on the system. Siemens recommends applying the Defense-in-Depth concept.

- Consult Siemens' product support documentation, or contact Siemens' customer service to determine if information on the compatibility of the updates provided by the vendors is available before applying the updates.

It is advised to configure the environment according to Siemens' operational guidelines [19] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] Siemens ProductCERT website:
https://www.siemens.com/cert/advisories

[2] Information from Google Project Zero:
https://googleprojectzero.blogspot.de/2018/01/reading-privileged-memory-with-side.html

[3] Information from researchers at TU Graz:
https://spectreattack.com/

[4] Information from Google Project Zero:
https://bugs.chromium.org/p/project-zero/issues/detail?id=1528

[5] Information from Cyberus Technology:
http://blog.cyberus-technology.de/posts/2018-06-06-intel-lazyfp-vulnerability.html

[6] Information from researchers at MIT and Carl Waldspurger Consulting:
https://arxiv.org/pdf/1807.03757.pdf

[7] Information from researchers regarding Foreshadow:
https://foreshadowattack.eu/

[8] Intel Security Advisory INTEL-SA-00088:
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

[9] Intel Security Advisory INTEL-SA-00115:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

[10] Intel Security Advisory INTEL-SA-00145:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00145.html

[11] Intel Security Advisory INTEL-OSS-10002:
https://01.org/security/advisories/intel-oss-10002

[12] Intel Security Advisory INTEL-SA-00161:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html

[13] Information from Microsoft:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV180002

[14] Information from Microsoft on Spectre Variant 3a:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV180013

[15] Information from Microsoft on Spectre Variant 4:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180012

[16] Information from Microsoft on Lazy FP State Restore:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180016

[17] Information from Microsoft on Spectre V1.1 (see Q23):
https://support.microsoft.com/en-ph/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

[18] Information from Microsoft on L1 Terminal Fault / Foreshadow:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv180018

[19] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[20] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[21] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-01-11):	Publication Date
V1.1 (2018-01-15):	Corrected CVE information
V1.2 (2018-05-29):	Added Spectre Variant 3a and Spectre Variant 4, summarized under Spectre-NG
V1.3 (2018-07-17):	Added Lazy FP State Restore and Spectre V1.1
V1.4 (2018-08-17):	Added L1 Terminal Fault / Foreshadow

DISCLAIMER