SSA-608355: Processor Vulnerabilities Affecting SIMATIC WinAC RTX (F) 2010

Publication Date: 2019-10-08
Last Update: 2019-10-08
Current Version: V1.0
CVSS v3.0 Base Score: 7.9

SUMMARY

Security researchers published information on vulnerabilities known as Spectre, Meltdown, Spectre-NG, Foreshadow, L1 Terminal Fault (L1TF), ZombieLoad, and Microarchitectural Data Sampling (MDS). These vulnerabilities affect many modern processors from different vendors to a varying degree.

The latest release of SIMATIC WinAC RTX provides compatibility with the latest BIOS updates and operating system patches from Intel and Microsoft.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinAC RTX (F) 2010: All versions < SIMATIC WinAC RTX 2010 SP3	Update to SIMATIC WinAC RTX 2010 SP3 and apply BIOS and Microsoft Windows updates https://support.industry.siemens.com/cs/ww/en/view/109765109

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- As a prerequisite 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.

  Siemens recommends limiting the possibilities to run untrusted code if possible.

- Applying a Defense-in-Depth concept can help to reduce the probability that untrusted code is run on the system. Siemens recommends to apply the Defense-in-Depth concept: https://www.siemens.com/industrialsecurity

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2017-5754

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2017-5715

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2017-5753

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3639

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3640

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3615

Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.

CVSS v3.0 Base Score	7.9
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3620

Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.

CVSS v3.0 Base Score	7.1
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3646

Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.

CVSS v3.0 Base Score	7.1
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-12126

Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-12127

Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-12130

Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2019-11091

Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVSS v3.0 Base Score	3.8
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2019-10-08): Publication Date

TERMS OF USE