SSA-168644: Spectre and Meltdown Vulnerabilities in Industrial Products

Publication Date: 2018-02-22
Last Update: 2018-04-18
Current Version: V1.3
CVSS v3.0 Base Score: 5.9

SUMMARY

Security researchers published information on vulnerabilities known as Spectre and Meltdown. These vulnerabilities affect many modern processors from different vendors to a varying degree.

Several Industrial Products include affected processors and are affected by the vulnerabilities.

AFFECTED PRODUCTS AND SOLUTION

For SIMATIC IPCs, SIMATIC Field PGs, SIMATIC ITP devices, SIMOTION P and SINUMERIK PCUs: Siemens provides first BIOS updates that include chipset microcode updates, and is working on further updates. In addition to applying the available BIOS updates, customers must also install the operating system patches that are provided by the operating system vendors in order to mitigate the vulnerabilities.

Siemens recommends to also follow the guidance from operating system vendors if such documentation was published. Microsoft, for example, published recommendations for Windows Servers:

https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

Affected Product and Versions	Remediation
RUGGEDCOM APE: All versions	Apply the available operating system updates for the operating system installed on the RUGGEDCOM APE as they become available. Until operating system patches are completely available, Siemens recommends to also apply the recommendations from section Workarounds and Mitigations.
RUGGEDCOM RX1400 VPE: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200 SP Open Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M4: All BIOS versions < V18.01.08	Update BIOS to V18.01.08 https://support.industry.siemens.com/cs/ww/en/view/109037537
SIMATIC Field PG M5: All BIOS versions < V22.01.05	Update BIOS to V22.01.05 or newer https://support.industry.siemens.com/cs/ww/en/view/109738122
SIMATIC HMI Basic Panels 2nd Generation: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC HMI Comfort 15-22 Panels (only MLFBs: 6AV2124-0QC02-0AX1, 6AV2124-1QC02-0AX1, 6AV2124-0UC02-0AX1, 6AV2124-0XC02-0AX1): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort 4-12" Panels: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort PRO Panels: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP Mobile Panels: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC227E: All BIOS versions < V20.01.11	Update BIOS to V20.0.11 https://support.industry.siemens.com/cs/ww/en/view/109481715
SIMATIC IPC277E: All BIOS versions < V20.01.11	Update BIOS to V20.0.11 https://support.industry.siemens.com/cs/ww/en/view/109481715
SIMATIC IPC3000 SMART V2: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC347E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC377E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC427C: All BIOS versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC427D: All BIOS versions < V17.0x.12	Update BIOS to V17.0x.12 https://support.industry.siemens.com/cs/ww/en/view/108608500
SIMATIC IPC427E: All BIOS versions < V21.01.08	Update BIOS to V21.01.08 https://support.industry.siemens.com/cs/ww/en/view/109742593
SIMATIC IPC477C: All BIOS versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477D: All BIOS versions < V17.0x.12	Update BIOS to V17.0x.12 https://support.industry.siemens.com/cs/ww/en/view/108608500
SIMATIC IPC477E: All BIOS versions < V21.01.08	Update BIOS to V21.01.08 https://support.industry.siemens.com/cs/ww/en/view/109742593
SIMATIC IPC477E Pro: All BIOS versions < V21.01.08	Update BIOS to V21.01.08 https://support.industry.siemens.com/cs/ww/en/view/109742593

SIMATIC IPC547E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC547G: All BIOS versions < R1.21.0	Update BIOS to R1.21.0 https://support.industry.siemens.com/cs/ww/en/view/109750349
SIMATIC IPC627C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC627D: All BIOS versions < V19.02.10	Update BIOS to V19.02.10 https://support.industry.siemens.com/cs/ww/en/view/109474954
SIMATIC IPC647D: All BIOS versions < V19.01.11	Update BIOS to V19.01.11 https://support.industry.siemens.com/cs/ww/en/view/109037779
SIMATIC IPC677C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC677D: All BIOS versions < V19.02.10	Update BIOS to V19.02.10 https://support.industry.siemens.com/cs/ww/en/view/109474954
SIMATIC IPC827C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC827D: All BIOS versions < V19.02.10	Update BIOS to V19.02.10 https://support.industry.siemens.com/cs/ww/en/view/109474954
SIMATIC IPC847C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC847D: All BIOS versions < V19.01.11	Update BIOS to V19.01.11 https://support.industry.siemens.com/cs/ww/en/view/109037779
SIMATIC ITP1000: All versions < V23.01.03	Update BIOS to V23.01.03 https://support.industry.siemens.com/cs/ww/en/view/109748173
SIMATIC S7-1500 Software Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1518-4 PN/DP ODK (MLFB: 6ES7518-4AP00-3AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1518F-4 PN/DP ODK (MLFB: 6ES7518-4FP00-3AB0): All versions	See recommendations from section Workarounds and Mitigations
SIMOTION P320-4E: All versions	See recommendations from section Workarounds and Mitigations
SIMOTION P320-4S: All versions	See recommendations from section Workarounds and Mitigations

SINEMA Remote Connect: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 840 D sl (NCU720.3B, NCU730.3B, NCU720.3, NCU730.3): All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK PCU 50.5: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK Panels wtih integrated TCU: All versions released >= 2016	Follow recommendations for SINUMERIK PCU or SINUMERIK TCU
SINUMERIK TCU 30.3: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- For SIMATIC IPCs, SIMATIC Field PGs, SIMATIC ITP devices, SIMOTION P and SINUMERIK PCUs: It is recommended to apply appropriate operating system updates while considering the compatiblity notes of the used application software. Applying the operating system patches provides mitigations against CVE-2017-5754 (Meltdown) and CVE-2017-5753 (Spectre Variant 1).

  Compatibility information for Siemens Industrial Software can be found at: https://support.industry.siemens.com/cs/ww/en/view/109754953

  Siemens recommends to also follow the guidance from operating system vendors if such documentation was published. Microsoft, for example, published recommendations for Windows Servers:

  https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

- 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 run the devices in a protected IT environment, Siemens particularly 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

RUGGEDCOM APE serves as a utility-grade computing platform for the RUGGEDCOM RX1500 router family. It also allows to run third party software applications without needing to procure an external industrial PC.

As the virtual machine environment for the RUGGEDCOM RX1400, the RUGGEDCOM VPE1400 is ideally suited for harsh environments, such as those found in electric power, transportation, defense systems and oil & gas industries.

The Siemens SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIMATIC Industrial PCs are the PC hardware platform for PC-based Automation from Siemens.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC Mobile Panel 277(F) IWLAN is designed for HMI tasks of medium complexity for wireless use in PROFINET environments.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

The Siemens SIMATIC S7-1500 ODK CPUs provide functionality of standard S7-1500 CPUs but additionally provide the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++. They have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMOTION is a scalable high performance hardware and software system for motion control.

SINEMA Remote Connect ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

SINUMERIK Panel Control Unit (PCU) offers HMI functionality for SINUMERIK CNC controllers.

SINUMERIK Thin Client Unit (TCU) offers HMI functionality for SINUMERIK CNC controllers.

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

ADDITIONAL INFORMATION

Further information on Spectre and Meltdown can be found on the website provided by the researchers: https://spectreattack.com/

Further information on SIMATIC IPC and SIMATIC Field PGs can be found on https://support.industry.siemens.com/cs/ww/en/view/109747626

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 (2018-02-22):	Publication Date
V1.1 (2018-03-15):	Corrected products: SIMATIC IPC3000 SMART V2, SIMATIC IPC647D. Added updates for SIMATIC IPC427E, IPC477E, IPC547G
V1.2 (2018-03-20):	Added updates for SIMATIC IPC647D, SIMATIC IPC847D, SIMATIC IPC627D, SIMATIC IPC677D, SIMATIC IPC827D, SIMATIC IPC227E, SIMATIC IPC277E
V1.3 (2018-04-18):	Added updates for SIMATIC IPC427D, SIMATIC IPC477D, SIMATIC FieldPG M4

TERMS OF USE