SSA-254686: Foreshadow / L1 Terminal Fault Vulnerabilities in Industrial Products

Publication Date: 2018-10-09
Last Update: 2018-12-11
Current Version: V1.2
CVSS v3.0 Base Score: 7.9

SUMMARY

Security researchers published information on vulnerabilities known as Foreshadow and L1 Terminal Fault (L1TF). These vulnerabilities affect many modern processors from different vendors to a varying degree.

Several Siemens Industrial Products contain processors that 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 the 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. Depending on the deployed operating system version, additional steps may be required to enable the mitigations. Please see operating system documentation for details.

Affected Product and Versions	Remediation
RUGGEDCOM APE: All versions	Apply Debian patches as they become available.
RUGGEDCOM RX1400 VPE: All versions	Apply Debian patches as they become available.
SIMATIC ET 200 SP Open Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200 SP Open Controller (F): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M4: All BIOS versions < V18.01.09	Update BIOS to V18.01.09 https://support.industry.siemens.com/cs/de/en/view/109037537
SIMATIC Field PG M5: All BIOS versions < V22.01.06	Update BIOS to V22.01.06 https://support.industry.siemens.com/cs/de/en/view/109738122
SIMATIC IPC227E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC277E: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC IPC3000 SMART V2: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC327E: 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 versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC427D: All BIOS versions < V17.0X.14	Update BIOS to V17.0X.14 https://support.industry.siemens.com/cs/de/en/view/108608500
SIMATIC IPC427E: All BIOS versions < V21.01.09	Update BIOS to V21.01.09 https://support.industry.siemens.com/cs/de/en/view/109742593
SIMATIC IPC477C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477D: All BIOS versions < V17.0X.14	Update BIOS to V17.0X.14 https://support.industry.siemens.com/cs/de/en/view/108608500
SIMATIC IPC477E: All BIOS versions < V21.01.09	Update BIOS to V21.01.09 https://support.industry.siemens.com/cs/de/en/view/109742593
SIMATIC IPC477E Pro: All BIOS versions < V21.01.09	Update BIOS to V21.01.09 https://support.industry.siemens.com/cs/de/en/view/109742593
SIMATIC IPC547E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC547G: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC627C: All BIOS versions < V15.02.15	Update BIOS to V15.02.15 https://support.industry.siemens.com/cs/ww/en/view/48792087
SIMATIC IPC627D: All BIOS versions < V19.02.11	Update BIOS to V19.02.11 https://support.industry.siemens.com/cs/ww/de/view/109474954
SIMATIC IPC647C: All BIOS version < V15.01.14	Update BIOS to V15.01.14 https://support.industry.siemens.com/cs/ww/en/view/48792076
SIMATIC IPC647D: All BIOS versions < V19.01.14	Update BIOS to V19.01.14 https://support.industry.siemens.com/cs/ww/en/view/109037779

SIMATIC IPC677C: All BIOS versions < V15.02.15	Update BIOS to V15.02.15 https://support.industry.siemens.com/cs/ww/en/view/48792087
SIMATIC IPC677D: All BIOS versions < V19.02.11	Update BIOS to V19.02.11 https://support.industry.siemens.com/cs/ww/de/view/109474954
SIMATIC IPC827C: All BIOS versions < V15.02.15	Update BIOS to V15.02.15 https://support.industry.siemens.com/cs/ww/en/view/48792087
SIMATIC IPC827D: All BIOS versions < V19.02.11	Update BIOS to V19.02.11 https://support.industry.siemens.com/cs/ww/de/view/109474954
SIMATIC IPC847C: All BIOS version < V15.01.14	Update BIOS to V15.01.14 https://support.industry.siemens.com/cs/ww/en/view/48792076
SIMATIC IPC847D: All BIOS versions < V19.01.14	Update BIOS to V19.01.14 https://support.industry.siemens.com/cs/ww/en/view/109037779
SIMATIC ITP1000: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU S7-1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0): All versions < V2.6	Update to V2.6 https://support.industry.siemens.com/cs/ww/en/view/109478459
SIMATIC S7-1500 CPU S7-1518F-4 PN/DP MFP (MLFB: 6ES7518-4FX00-1AC0): All versions < V2.6	Update to V2.6 https://support.industry.siemens.com/cs/ww/en/view/109478459
SIMATIC S7-1500 Software Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMOTION P320-4E: All BIOS versions < V17.0X.14	Update BIOS to V17.0X.14 https://support.industry.siemens.com/cs/de/en/view/108608500
SIMOTION P320-4S: All BIOS versions < V17.0X.14	Update BIOS to V17.0X.14 https://support.industry.siemens.com/cs/de/en/view/108608500
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:

- As a prerequisite for an attack, an attacker must be able to run untrusted code on affected systems. 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

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 and gas industries.

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

The 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.

The SIMATIC S7-1500 MFP CPUs provide functionality of standard S7-1500 CPUs with the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++ and an additional second independent runtime environment to execute C/C++ applications parallel to the Step 7 program if required.

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-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

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 (2018-10-09):	Publication Date
V1.1 (2018-11-13):	Added solution for SIMATIC IPC647D, SIMATIC IPC847D, SIMATIC IPC647C, SIMATIC IPC847C, SIMATIC IPC627C, SIMATIC IPC677C, SIMATIC IPC827C, SIMOTION P320-4S, SIMOTION P320-4E
V1.2 (2018-12-11):	Added solution for SIMATIC IPC627D, SIMATIC IPC677D, SIMATIC IPC827D

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License

Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.