SSA-616472: ZombieLoad and Microarchitectural Data Sampling Vulnerabilities in Industrial Products

Publication Date: 2019-07-09
Last Update: 2020-12-08
Current Version: V1.7
CVSS v3.1 Base Score: 6.5

SUMMARY

Security researchers published information on vulnerabilities known as ZombieLoad and Microarchitectural Data Sampling (MDS). 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
SIMATIC Field PG M4: All BIOS versions < V18.01.09	Update BIOS to V18.01.09 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC Field PG M5: All BIOS versions < V22.01.07	Update BIOS to V22.01.07 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC Field PG M6: All BIOS versions < V26.01.05	Update BIOS to V26.01.05 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC127E: All BIOS versions < V27.01.04	Update BIOS to V27.01.04 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC2X7E: All BIOS versions < V20.01.13	Update BIOS to V20.01.13 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC3000 SMART V2: All versions < V1.7	Update BIOS to V1.7 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC327E: All BIOS versions < V1.7	Update BIOS to V1.7 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC347E: All versions < V1.7	Update BIOS to V1.7 https://support.industry.siemens.com/cs/ww/en/view/109763408

SIMATIC IPC377E: All BIOS versions < V1.7	Update BIOS to V1.7 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC427C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC427D (incl. SIPLUS variants): All BIOS versions < V17.0X.16	Update BIOS to V17.0X.16 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC427E (incl. SIPLUS variants): All BIOS versions < V21.01.11	Update BIOS to V21.01.11 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC477C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477D: All BIOS versions < V17.0X.16	Update BIOS to V17.0X.16 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC477E: All BIOS versions < V21.01.11	Update BIOS to V21.01.11 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC477E Pro: All BIOS versions < V21.01.11	Update BIOS to V21.01.11 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC527G: All BIOS versions < V1.3.0	Update BIOS to V1.3.0 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC547E: All BIOS versions < R1.33	Update BIOS to R1.33 https://support.industry.siemens.com/cs/us/en/view/109763408
SIMATIC IPC547G: All BIOS versions < R1.24.0	Update BIOS to R1.24.0 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC627C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC627D: All BIOS versions < V19.02.12	Update BIOS to V19.02.12 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC627E: All BIOS versions < V25.02.04	Update BIOS to V25.02.04 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC647C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC647D: All BIOS versions < V19.01.15	Update BIOS to V19.01.15 https://support.industry.siemens.com/cs/ww/en/view/109763408

SIMATIC IPC647E: All BIOS versions < V25.02.04	Update BIOS to V25.02.04 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC677C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC677D: All BIOS versions < V19.02.12	Update BIOS to V19.02.12 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC677E: All BIOS versions < V25.02.04	Update BIOS to V25.02.04 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC827C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC827D: All BIOS versions < V19.02.12	Update BIOS to V19.02.12 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC847C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC847D: All BIOS versions < V19.01.15	Update BIOS to V19.01.15 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC847E: All BIOS versions < V25.02.04	Update BIOS to V25.02.04 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC ITP1000: All BIOS versions < V23.01.06	Update BIOS to V23.01.06 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0, 6AG1518-4AX00-4AC0, incl. SIPLUS variant): All versions < V2.8.4	Update to V2.8.4 https://support.industry.siemens.com/cs/ww/en/view/109761490
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (MLFB: 6ES7518-4FX00-1AC0): All versions < V2.8.4	Update to V2.8.4 https://support.industry.siemens.com/cs/ww/en/view/109761495
SIMOTION P320-4E: All BIOS versions < V17.0X.16	Update BIOS to V17.0X.16 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMOTION P320-4S: All BIOS versions < V17.0X.16	Update BIOS to V17.0X.16 https://support.industry.siemens.com/cs/ww/en/view/109763408
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 with integrated TCU: All versions released	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

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

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.

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.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

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 v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 v3.1 Base Score	3.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2019-07-09):	Publication Date
V1.1 (2019-08-13):	Updated link for SIMATIC IPCs 427D, 477D, 627D, 627E, 647D, 647E, 677D, 677E, 827D, 847D, 847E and FieldPG M6
V1.2 (2019-09-10):	Updates for FieldPG M4, FieldPG M5 and ITP1000
V1.3 (2019-11-12):	Updates for SIMOTION P320-4E, SIMOTION P320-4S and SIMATIC IPC547G
V1.4 (2019-12-10):	Updates for SIMATIC IPC2X7E, SIMATIC IPC327E, SIMATIC IPC377E, and SIPLUS devices now explicitly mentioned in the list of affected products
V1.5 (2020-02-11):	Updates for SIMATIC IPC547E, SIMATIC IPC347E, and SIMATIC IPC3000 SMART V2
V1.6 (2020-03-10):	Updates for SIMATIC IPC127E, and SIMATIC IPC527G
V1.7 (2020-12-08):	Remove wrong MLFB from SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP and Updates for SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP

TERMS OF USE