SSA-534763: Special Register Buffer Data Sampling (SRBDS) aka Crosstalk in Industrial Products

Publication Date: 2020-09-08
Last Update: 2022-03-08
Current Version: V1.6
CVSS v3.1 Base Score: 5.5

SUMMARY

Security researchers published information on a vulnerability known as Crosstalk (INTEL-SA-00320). This vulnerability affects modern Intel processors to a varying degree.

Several Siemens Industrial Products contain processors that are affected by the vulnerability.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Field PG M4: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M5: All BIOS versions < V22.01.08	Update BIOS to V22.01.08 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC Field PG M6: All BIOS versions < V26.01.07	Update BIOS to V26.01.07 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC347E: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC427D (incl. SIPLUS variants): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC427E (incl. SIPLUS variants): All BIOS versions < V21.01.14	Update BIOS to V21.01.14 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC477D: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SIMATIC IPC477E: All BIOS versions < V21.01.14	Update BIOS to V21.01.14 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All BIOS versions < V21.01.14	Update BIOS to V21.01.14 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC527G: All BIOS versions < V1.4.0	Update BIOS to V1.4.0 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC547E: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC547G: All BIOS versions < R1.28.0	Update BIOS to R1.28.0 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC627D: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All BIOS versions < V25.02.06	Update BIOS to V25.02.06 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC647D: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All BIOS versions < V25.02.06	Update BIOS to V25.02.06 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC677D: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All BIOS versions < V25.02.06	Update BIOS to V25.02.06 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC827D: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations

SIMATIC IPC847D: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All BIOS versions < V25.02.06	Update BIOS to V25.02.06 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC3000 SMART V2: All versions < V1.B	Update BIOS to V1.B or later version https://support.industry.siemens.com/cs/cn/en/view/109763408/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITP1000: All BIOS versions < V23.01.08	Update BIOS to V23.01.08 https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMOTION P320-4E: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMOTION P320-4S: All versions	Currently no remediation is planned 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 Field PG is a mobile, industry-standard programming device for automation engineers with all commonly used interfaces for industrial applications that also brings pre-installed SIMATIC engineering software.

SIMATIC IPC (Industrial PC) is the hardware platform for PC-based automation from Siemens.

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

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-2020-0543

Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 (2020-09-08):	Publication Date
V1.1 (2020-10-13):	Removed SINUMERIK 840D sl (NCU730.3B), SINUMERIK 828D (PPU.4 / PPU1740), and SINUMERIK ONE (NCU1750 / NCU1760) from the list of affected products. Added solution for SIMATIC IPC627E, SIMATIC IPC647E, SIMATIC IPC677E, and SIMATIC IPC847E
V1.2 (2020-12-08):	Added solution for SIMATIC IPC427E, SIMATIC IPC477E, and SIMATIC IPC477E PRO
V1.3 (2021-02-09):	Added solution for SIMATIC Field PG M5, and SIMATIC Field PG M6
V1.4 (2021-04-13):	Added solution for SIMATIC ITP1000 and SIMATIC IPC547G
V1.5 (2021-06-08):	Added solution for SIMATIC IPC527G
V1.6 (2022-03-08):	Added solution for SIMATIC IPC3000 SMART V2 and clarified that no further fixes are planned

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.