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

Publication Date: 2020-09-08
Last Update: 2020-09-08
Current Version: V1.0
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 is preparing updates and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Field PG M4: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M5: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M6: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC3000 SMART: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC347E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC427D (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC427E (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477D: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC527G: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC IPC547E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC547G: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC627D: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC647D: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC677D: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC827D: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC847D: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITP1000: 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
SINUMERIK 828D (PPU.4 / PPU1740): All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 840D sl (NCU730.3B): All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK ONE (NCU1750 / NCU1760): 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.

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.

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

TERMS OF USE