

SSA-678983: Vulnerabilities in Industrial PCs and CNC devices using Intel CPUs (November 2020)

Publication Date: 2021-05-11
 Last Update: 2022-12-13
 Current Version: V1.6
 CVSS v3.1 Base Score: 7.8

SUMMARY

Intel has published information on vulnerabilities in Intel products in [November 2020](#). This advisory lists the Siemens IPC related products, that are affected by these vulnerabilities.

In this advisory we take a representative CVE from each advisory:

- “Intel CSME, SPS, TXE, AMT and DAL Advisory” Intel-SA-00391 is represented by CVE-2020-8745
- “Intel RAPL Interface Advisory” Intel-SA-00389 is represented by CVE-2020-8694
- “Intel Processor Advisory” Intel-SA-00381 is represented by CVE-2020-8698, and
- “BIOS Advisory” Intel-SA-00358 is represented by CVE-2020-0590.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller family: All versions < V05.00.01.00 only affected by CVE-2020-8745	Update BIOS to V05.00.01.00 or later version The update can be obtained from your local Siemens account manager. See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V0209_0105 only affected by CVE-2020-8745	Update BIOS to V0209_0105 or later version https://support.industry.siemens.com/cs/ww/en/view/109743969/ See further recommendations from section Workarounds and Mitigations
SIMATIC Field PG M5: All BIOS versions < V22.01.08 only affected by CVE-2020-8694, CVE-2020-8698, CVE-2020-8745	Update BIOS to V22.01.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC Field PG M6: All versions < V26.01.08 only affected by CVE-2020-0590, CVE-2020-8694, CVE-2020-8698, CVE-2020-8745	Update BIOS to V26.01.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC127E: All versions only affected by CVE-2020-8745	Update BIOS to V27.01.05 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations

<p>SIMATIC IPC427E (incl. SIPLUS variants): All BIOS versions < V21.01.15 only affected by CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V21.01.15 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC477E: All BIOS versions < V21.01.15 only affected by CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V21.01.15 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC477E Pro: All BIOS versions < V21.01.15 only affected by CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V21.01.15 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC527G: All BIOS versions < V1.4.0 only affected by CVE-2020-0590, CVE-2020-8694, CVE-2020-8745</p>	<p>Update BIOS to V1.4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC547G: All versions < R1.30.0 only affected by CVE-2020-0590, CVE-2020-8694</p>	<p>Update BIOS to R1.30.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC627E: All BIOS versions < V25.02.08 only affected by CVE-2020-0590, CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V25.02.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC647E: All BIOS versions < V25.02.08 only affected by CVE-2020-0590, CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V25.02.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC677E: All BIOS versions < V25.02.08 only affected by CVE-2020-0590, CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V25.02.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC IPC847E: All BIOS versions < V25.02.08 only affected by CVE-2020-0590, CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V25.02.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>
<p>SIMATIC ITP1000: All BIOS versions < V23.01.08 only affected by CVE-2020-8694, CVE-2020-8698, CVE-2020-8745</p>	<p>Update BIOS to V23.01.08 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations</p>

SINUMERIK 828D HW PU.4: All Versions < V08.00.00.00 only affected by CVE-2020-8745	Update BIOS to V08.00.00.00 or later version SINUMERIK software can be obtained from your local Siemens account manager. See further recommendations from section Workarounds and Mitigations
SINUMERIK MC MCU 1720: All versions < V05.00.00.00 only affected by CVE-2020-8745	Update BIOS to V05.00.00.00 or later version SINUMERIK software can be obtained from your local Siemens account manager. See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE / SINUMERIK 840D sl Hand-held Terminal HT 10: All versions < V08.00.00.00 only affected by CVE-2020-8745	Update BIOS to V08.00.00.00 or later version SINUMERIK software can be obtained from your local Siemens account manager. See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE NCU 1740: All versions < V04.00.00.00 only affected by CVE-2020-8745	Update BIOS to V04.00.00.00 or later version SINUMERIK software can be obtained from your local Siemens account manager. See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE PPU 1740: All versions < V06.00.00.00 only affected by CVE-2020-8745	Update BIOS to V06.00.00.00 or later version SINUMERIK software can be obtained from your local Siemens account manager. See further 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>

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). Please follow the [General Security Recommendations](#).

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 Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

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

The SIMATIC Tablet PC ITP1000 offers the performance of SIMATIC industrial PCs in a tablet format

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-2020-0590

Improper input validation in BIOS firmware for some Intel Processors may allow an authenticated user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-8694

Insufficient access control in the Linux kernel driver for some Intel Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2020-8698

Improper isolation of shared resources in some Intel 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-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC)

Vulnerability CVE-2020-8745

Insufficient control flow management in subsystem for Intel(R) CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25 , Intel(R) TXE versions before 3.1.80 and 4.0.30 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.

CVSS v3.1 Base Score 6.8
CVSS Vector [CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C](#)
CWE CWE-269: Improper Privilege Management

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 (2021-05-11): Publication Date
V1.1 (2021-06-08): Added remediations for SIMATIC IPC427E, SIMATIC IPC477E (PRO), and SIMATIC IPC527G
V1.2 (2021-08-10): Added remediations for SIMATIC IPC127E, SINUMERIK 828D HW PU.4, SINUMERIK MC MCU 1720, SINUMERIK ONE NCU 1740 and SINUMERIK ONE PPU 1740, added SIMATIC Drive Controller
V1.3 (2022-03-08): Added solution for SIMATIC ET 200SP Open Controller CPU 1515SP PC2
V1.4 (2022-05-10): Added solution for SIMATIC IPC547G
V1.5 (2022-07-12): Added fix for SIMATIC Field PG M6
V1.6 (2022-12-13): Added fix for SINUMERIK ONE / 840D sl Handheld Terminal HT 10

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.