

## SSA-398519: Vulnerabilities in Intel CPUs (November 2019)

Publication Date: 2020-02-11  
 Last Update: 2021-03-09  
 Current Version: V1.6  
 CVSS v3.1 Base Score: 9.6

### SUMMARY

Intel has published information on vulnerabilities in Intel products in [November 2019](#). In this advisory Siemens only explicitly mentions the vulnerabilities from the “Intel® CPU Security Advisory” and one vulnerability from “Intel® CSME, Intel® SPS, Intel® TXE, Intel® AMT, Intel® PTT and Intel® DAL Advisory” and lists the Siemens IPC related products that are affected by these vulnerabilities. For further information about BIOS updates related to Intel CPU vulnerabilities see: <https://support.industry.siemens.com/cs/ww/en/view/109747626>.

Several Siemens Industrial Products contain processors that are affected by the vulnerabilities. Siemens has released updates for several affected products and is currently working on BIOS updates that include chipset microcode updates for further products.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All BIOS versions < V2.08 only affected by CVE-2019-0169	Update BIOS to V2.08 <a href="https://support.industry.siemens.com/cs/ww/en/view/109743969">https://support.industry.siemens.com/cs/ww/en/view/109743969</a>
SIMATIC Field PG M4: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC Field PG M5: All BIOS versions < V22.01.08 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to V22.01.08 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC Field PG M6: All BIOS versions < V26.01.07 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to V26.01.07 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC127E: All BIOS versions < V27.01.04 only affected by CVE-2019-0169	Update BIOS to V27.01.04 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC427C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC427D (incl. SIPLUS variants): All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>

SIMATIC IPC427E (incl. SIPLUS variants): All BIOS versions < V21.01.13 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to V21.01.13 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC477C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC477D: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC477E: All BIOS versions < V21.01.13 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to V21.01.13 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC477E Pro: All BIOS versions < V21.01.13 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to V21.01.13 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC527G: All BIOS versions < V1.3.2 only affected by CVE-2019-0169	Update BIOS to V1.3.2 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC547E: All BIOS versions < R1.34 only affected by CVE-2019-0151	Update BIOS to R1.34 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC547G: All BIOS versions < R1.28.0 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to R1.28.0 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC627C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC627D: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC627E: All BIOS versions < V25.02.05	Update BIOS to V25.02.05 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC647C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC647D: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>

SIMATIC IPC647E: All BIOS versions < V25.02.05	Update BIOS to V25.02.05 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC677C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC677D: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC677E: All BIOS versions < V25.02.05	Update BIOS to V25.02.05 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC IPC827C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC827D: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC847C: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC847D: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC847E: All BIOS versions < V25.02.05	Update BIOS to V25.02.05 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMATIC ITP1000: All BIOS versions < V23.01.07 only affected by CVE-2019-0151, CVE-2019-0169	Update BIOS to V23.01.07 <a href="https://support.industry.siemens.com/cs/ww/en/view/109763408">https://support.industry.siemens.com/cs/ww/en/view/109763408</a>
SIMOTION P320-4E: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMOTION P320-4S: All versions only affected by CVE-2019-0151	See recommendations from section <a href="#">Workarounds and Mitigations</a>

## **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.

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-2019-0151

Insufficient memory protection in Intel(R) TXT for certain Intel(R) Core Processors and Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	7.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

### Vulnerability CVE-2019-0152

Insufficient memory protection in System Management Mode (SMM) and Intel(R) TXT for certain Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	8.2
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

### Vulnerability CVE-2019-0169

Heap overflow in subsystem in Intel(R) CSME; Intel(R) TXE could allow an unauthenticated user to potentially enable escalation of privileges, information disclosure or denial of service via adjacent access.

CVSS v3.1 Base Score	9.6
CVSS Vector	<a href="#">CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-122: Heap-based Buffer Overflow

### **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 (2020-02-11): Publication Date  
V1.1 (2020-03-10): Updated solution for SIMATIC IPC127E, SIMATIC IPC627E, SIMATIC IPC647E, SIMATIC IPC677E, and SIMATIC IPC847E  
V1.2 (2020-04-14): Updated solution for SIMATIC ET 200SP Open Controller CPU 1515SP PC2  
V1.3 (2020-07-14): Updated solution for SIMATIC ITP1000; removed SIMATIC IPC827E from list of affected devices, as it was not publicly released  
V1.4 (2020-10-13): Updated solution for SIMATIC IPC427E, SIMATIC IPC477E, and SIMATIC IPC477E Pro  
V1.5 (2021-02-09): Updated solution for SIMATIC IPC527G, SIMATIC Field PG M5, and SIMATIC Field PG M6  
V1.6 (2021-03-09): Updated solution for SIMATIC IPC547E and SIMATIC IPC547G

### **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](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.