SSA-309571: IPU 2021.1 Vulnerabilities in Siemens Industrial Products using Intel CPUs (June 2021)

Publication Date: 2021-08-10
Last Update: 2021-08-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

Intel has published information on vulnerabilities in Intel products in June 2021. This advisory lists the related Siemens Industrial products affected by these vulnerabilities that can be patched by applying the corresponding BIOS update.

In this advisory we summarize:

- “2021.1 IPU – Intel® CSME, SPS and LMS Advisory” Intel-SA-00459,
- “2021.1 IPU – BIOS Advisory” Intel-SA-00463,
- “2021.1 IPU – Intel® Processor Advisory” Intel-SA-00464, and
- “2021.1 IPU - Intel Atom® Processor Advisory” Intel-SA-00465.

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 Drive Controller family: All versions only affected by CVE-2020-24513	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions only affected by CVE-2020-24513	See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M5: All versions only affected by CVE-2020-24507, CVE-2020-24512, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC Field PG M6: All versions only affected by CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC IPC127E: All versions only affected by CVE-2020-24513	See recommendations from section Workarounds and Mitigations

SIMATIC IPC427E: All versions only affected by CVE-2020-12357, CVE-2020-24507, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E: All versions only affected by CVE-2020-12357, CVE-2020-24507, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All versions only affected by CVE-2020-12357, CVE-2020-24507, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC IPC527G: All versions only affected by CVE-2020-24507, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC IPC547G: All versions only affected by CVE-2020-12357, CVE-2020-12358, CVE-2020-12360, CVE-2020-24486, CVE-2020-24507, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC IPC627E: All BIOS versions < V25.02.10 only affected by CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	Update BIOS to V25.02.10 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC647E: All BIOS versions < V25.02.10 only affected by CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	Update BIOS to V25.02.10 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC IPC677E: All BIOS versions < V25.02.10 only affected by CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	Update BIOS to V25.02.10 https://support.industry.siemens.com/cs/ww/en/view/109763408

SIMATIC IPC847E: All BIOS versions < V25.02.10 only affected by CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	Update BIOS to V25.02.10 https://support.industry.siemens.com/cs/ww/en/view/109763408
SIMATIC ITP1000: All versions only affected by CVE-2020-12357, CVE-2020-24507, CVE-2020-24512, CVE-2020-8670, CVE-2020-8703, CVE-2020-8704	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0, 6AG1518-4AX00-4AC0, incl. SIPLUS variant): All versions only affected by CVE-2020-12357, CVE-2020-12360	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (MLFB: 6ES7518-4FX00-1AC0): All versions only affected by CVE-2020-12357, CVE-2020-12360	See recommendations from section Workarounds and Mitigations
SINUMERIK 828D HW PU.4: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK MC MCU 1720: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK ONE / SINUMERIK 840D sl Handheld Terminal HT 10: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK ONE PPU 1740: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific mitigations or workarounds. Please follow General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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

Products of the SIMATIC Drive Controller family 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 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 Industrial PCs are the PC hardware platform for PC-based Automation from Siemens.

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.

The 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.

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.

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

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-2020-8670

Race condition in the firmware for some Intel(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	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-8703

Improper buffer restrictions in a subsystem in the Intel(R) CSME versions before 11.8.86, 11.12.86, 11.22.86, 12.0.81, 13.0.47, 13.30.17, 14.1.53, 14.5.32 and 15.0.22 may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	5.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-8704

Race condition in a subsystem in the Intel(R) LMS versions before 2039.1.0.0 may allow a privileged user to potentially enable escalation of privilege via local access.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-12357

Improper initialization in the firmware for some Intel(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	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-12358

Out of bounds write in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-12360

Out of bounds read in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege 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:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-24486

Improper input validation in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable denial of service 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:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-24506

Out of bound read in a subsystem in the Intel(R) CSME versions before 12.0.81, 13.0.47, 13.30.17, 14.1.53 and 14.5.32 may allow a privileged user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-24507

Improper initialization in a subsystem in the Intel(R) CSME versions before 11.8.86, 11.12.86, 11.22.86, 12.0.81, 13.0.47, 13.30.17, 14.1.53, 14.5.32, 13.50.11 and 15.0.22 may allow a privileged user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	6.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-24511

Improper isolation of shared resources in some Intel(R) 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:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-24512

Observable timing discrepancy in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	2.8
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2020-24513

Domain-bypass transient execution vulnerability in some Intel Atom(R) 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:U/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

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 (2021-08-10): Publication Date

TERMS OF USE