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

Publication Date: 2021-08-10
Last Update: 2024-02-13
Current Version: V2.0
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 new versions for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions affected by CVE-2020-24513	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions affected by CVE-2020-24513	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V0209_0105 affected by CVE-2020-24513	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 versions < V22.01.10 affected by CVE-2020-8703, CVE-2020-8704, CVE-2020-24507, CVE-2020-24512	Update BIOS to V22.01.10 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 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512	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 < V27.01.07 affected by CVE-2020-24513	Update BIOS to V27.01.07 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC347G: All versions < V01.04.00 affected by all CVEs	Update BIOS to V01.04.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC427E: All versions < V21.01.16 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24507, CVE-2020-24512	Update BIOS to V21.01.16 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC477E: All versions < V21.01.16 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24507, CVE-2020-24512	Update BIOS to V21.01.16 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC477E Pro: All versions < V21.01.16 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24507, CVE-2020-24512	Update BIOS to V21.01.16 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC527G: All versions < V1.4.3 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-24507, CVE-2020-24512	Update BIOS to V1.4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC547G: All versions affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-12358, CVE-2020-12360, CVE-2020-24486, CVE-2020-24507, CVE-2020-24512	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC IPC627E: All BIOS versions < V25.02.10 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512	Update BIOS to V25.02.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC647E: All BIOS versions < V25.02.10 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512	Update BIOS to V25.02.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC677E: All BIOS versions < V25.02.10 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512	Update BIOS to V25.02.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC847E: All BIOS versions < V25.02.10 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24506, CVE-2020-24507, CVE-2020-24511, CVE-2020-24512	Update BIOS to V25.02.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC3000 SMART V3: All versions < V01.04.00 affected by all CVEs	Update BIOS to V01.04.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC ITP1000: All versions < V23.01.10 affected by CVE-2020-8670, CVE-2020-8703, CVE-2020-8704, CVE-2020-12357, CVE-2020-24507, CVE-2020-24512	Update BIOS to V23.01.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109763408 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP family (incl. SIPLUS variant): All versions affected by CVE-2020-12357, CVE-2020-12360	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AC0): All versions affected by CVE-2020-12357, CVE-2020-12360	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINUMERIK 828D HW PU.4: All versions < V08.00.00.00 affected by all CVEs	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 affected by all CVEs	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 Handheld Terminal HT 10: All versions < V08.00.00.00 affected by all CVEs	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 < V05.00.00.00 affected by all CVEs	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 PPU 1740: All versions < V06.00.00.00 affected by all CVEs	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.

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 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.

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.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

SINUMERIK MC is a CNC system for customized machine solutions.

SINUMERIK ONE is a digital-native CNC system with an integrated SIMATIC S7-1500 CPU for automation.

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

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
V1.1 (2022-02-08):	Added affected product SINUMERIK ONE NCU 1740
V1.2 (2022-03-08):	Added mitigation; clarified no remediation planned for SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP; added solution for SIMATIC IPC127E and SIMATIC ET 200SP Open Controller CPU 1515SP PC2
V1.3 (2022-04-12):	Added solution for SIMATIC IPC427E, SIMATIC IPC 477E, and SIMATIC IPC477E PRO
V1.4 (2022-07-12):	Added fix for SIMATIC ITP1000 and SIMATIC Field PG M6
V1.5 (2022-08-09):	Added SIMATIC IPC347G and SIMATIC SMART V3 to the list of affected products
V1.6 (2022-09-13):	Added fix for SIMATIC IPC347G and SIMATIC IPC3000 SMART V3
V1.7 (2022-12-13):	Added fix for SINUMERIK 828D HW PU.4, SINUMERIK MC MCU 1720, SINUMERIK ONE / 840D sl Handheld Terminal HT 10, SINUMERIK ONE PPU 1740
V1.8 (2023-05-09):	Updated fix for SIMATIC IPC127E, added fix for SIMATIC Field PG M5
V1.9 (2023-11-14):	Added no fix planned for SIMATIC IPC547G
V2.0 (2024-02-13):	Added fix for SIMATIC IPC527G

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.