SSA-874235: Intel Vulnerability in Siemens Industrial Products

Publication Date: 2017-06-26
Last Update: 2020-02-10
Current Version: V1.4
CVSS v3.1 Base Score: 9.8

SUMMARY

Several Intel chipsets for Intel Core i5, Intel Core i7 and Intel XEON are susceptible to remote code execution vulnerability (CVE-2017-5689) [1]. As several Siemens Industrial Products use Intel technology, they are also affected. Siemens has released updates for the affected Industrial PCs.

[1] Intel Security Advisory – INTEL-SA-00075:https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Customized IPCs: Customized versions	For those devices, customers will be informed directly by Siemens.
Field PG M3: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
Field PG M4: BIOS < V18.01.06	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
Field PG M5: BIOS < V22.01.03	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
IPC627D / IPC677D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC427D: BIOS < V17.0?.10	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC427E: BIOS < V21.01.04	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC477D: BIOS < V17.0?.10	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC547D: ME < V7.1.91.3272	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC547E: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626

PCS 7 IPC547G: ME < V11.0.26.3000	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC627C / IPC677C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC647C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC647D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC847C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
PCS 7 IPC847D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC427D (incl. SIPLUS variants): BIOS < V17.0?.10	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC427E (incl. SIPLUS variants): BIOS < V21.01.05	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC477D: BIOS < V17.0?.10	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC477D PRO: BIOS < V17.0?.10	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC477E: BIOS < V21.01.05	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC547D: ME < V7.1.91.3272	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC547E: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC547G: ME < V11.0.26.3000	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC627C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC627D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626

SIMATIC IPC647C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC647D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC677C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC677D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC827C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC827D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC847C: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC IPC847D: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMATIC ITP1000: ME < V9.1.41.3024	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SIMOTION P320-4 Standard: BIOS < S17.02.06.83.1	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626
SINUMERIK PCU50.5-P: ME < V6.2.61.3535	Update firmware https://support.industry.siemens.com/cs/ww/en/view/109747626

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- 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.

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.

SINUMERIK Panel Control Unit (PCU) offers HMI functionality for SINUMERIK CNC controllers.

SIMOTION P320 is an Industrial PC for motion control.

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-2017-5689

Unprivileged local or remote attackers can gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM) and Intel Small Business Technology (SBT).

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2017-06-26):	Publication Date
V1.1 (2017-06-29):	Minor changes
V1.2 (2017-07-06):	Removed two SINUMERIK from affected products section, added new updates
V1.3 (2017-07-13):	Updates for all products available
V1.4 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.