# SSA-874235: Intel Vulnerability in Siemens Industrial Products

Publication Date 2017-06-26
Last Update 2017-07-13
Current Version V1.3
CVSS v3.0 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.

## AFFECTED PRODUCTS

| SIMATIC IPC | MLFB | Affected version |
|---|---|---|
| IPC427D | 6AG4140-6*, 6AG4140-7*, 6AG4140-8* | BIOS < V17.0?.10 |
| IPC477D | 6AV7240-6*, 6AV7240-7*, 6AV7240-8* 6AV7244-5EA02-0HB0, 6AV7244-5DA30-0YA0, 6AV7244-5DA30-0YB0 | BIOS < V17.0?.10 |
| IPC477D PRO | 6AV7250-6*, 6AV7250-7*, 6AV7250-8* | BIOS < V17.0?.10 |
| IPC427E | 6AG4141-5*, 6AG4141-7* | BIOS < V21.01.05 |
| IPC477E | 6AV7241-5*, 6AV7241-7* | BIOS < V21.01.05 |
| IPC547D | 6AG4104-2C*, 6AG4104-2D* | ME < V7.1.91.3272 |
| IPC547E | 6AG4104-3H*, 6AG4104-3K* | ME < V9.1.41.3024 |
| IPC547G | 6AG4104-4G*, 6AG4104-4H*, 6AG4104-4J* | ME < V11.0.26.3000 |
| IPC627C | 6ES7647-6CG*, 6ES7647-6CH*, 6ES7647-6CJ* | ME < V6.2.61.3535 |
| IPC647C | 6AG4112-1K* to 6AG4112-1N*, 6AG4112-1P*, 6AG4112-1R* | ME < V6.2.61.3535 |
| IPC677C | 6AV789?-??G*, 6AV789?-?H*, 6AV789?-??J* | ME < V6.2.61.3535 |
| IPC627D | 6AG4131-2G*, 6AG4131-2H*, 6AG4131-2J* | ME < V9.1.41.3024 |
| IPC647D | 6AG4112-2J* to 6AG4112-2M* 6AG4112-2G*, 6AG4112-2H* | ME < V9.1.41.3024 |
| IPC677D | 6AV7260-?G*, 6AV7260-?H*, 6AV7260-?J* | ME < V9.1.41.3024 |
| IPC827C | 6ES7647-6PG*, 6ES7647-6PH*, 6ES7647-6PJ* | ME < V6.2.61.3535 |
| IPC847C | 6AG4114-1K* to 6AG4114-1N*, 6AG4114-1P*, 6AG4114-1R* | ME < V6.2.61.3535 |
| IPC827D | 6AG4132-2G*, 6AG4132-2H*, 6AG4132-2J* | ME < V9.1.41.3024 |
| IPC847D | 6AG4114-2J* to 6AG4114-2N*, 6AG4114-2G*, 6AG4114-2H*, 6AG4114-2P*, 6AG4114-2Q* | ME < V9.1.41.3024 |

| | | |
|---|---|---|
| ITP1000 | 6AV7880-0????2* | BIOS < V23.01.02 |

| Field PG | MLFB | Affected version |
|---|---|---|
| Field PG M3 | 6ES7715-1BB*, 6ES7715-1CC* | ME < V6.2.61.3535 |
| Field PG M4 | 6ES7716-1*, 6ES7716-2* | BIOS < V18.01.06 |
| Field PG M5 | 6ES7717-0*, 6ES7717-1* | BIOS < V22.01.03 |

| PCS 7 IPC | MLFB | Affected version |
|---|---|---|
| IPC547D | 6ES7660-3*, 6ES7650-0TH17-0YX0 | ME < V7.1.91.3272 |
| IPC547E | 6ES7660-4* | ME < V9.1.41.3024 |
| IPC547G | 6ES7660-7* | ME < V11.0.26.3000 |
| IPC647C | 6ES7660-1* | ME < V6.2.61.3535 |
| IPC647D | 6ES7660-5* | ME < V9.1.41.3024 |
| IPC847C | 6ES7660-2* | ME < V6.2.61.3535 |
| IPC847D | 6ES7660-6* | ME < V9.1.41.3024 |
| IPC627C / IPC677C | 6ES7650-4A*, 6EQ2020-0AC03-5XX0 | ME < V6.2.61.3535 |
| IPC627D / IPC677D | 6ES7650-4B* | ME < V9.1.41.3024 |
| IPC427D | 6ES7650-0UG??-0YX?, 6ES7654-0UE23-0XX? | BIOS < V17.0?.10 |
| IPC427E | 6ES7650-0RJ02-0YX0 | BIOS < V21.01.04 |
| IPC477D | 6ES7650-0UG??-1YX? | BIOS < V17.0?.10 |

| Motion control | MLFB | Affected version |
|---|---|---|
| SINUMERIK PCU50.5-P | 6FC5210-0DF53-2AA0<br>6FC5210-0DF53-3AA0 | ME < V6.2.61.3535 |
| SIMOTION P320-4 Standard | 6AU1320-4DS66-3AG0 | BIOS < S17.02.06.83.1 |

Customized versions of the listed SIMATIC IPCs may also be affected. For these devices, customers will be informed directly by Siemens.

## DESCRIPTION

SIMATIC Industrial PCs are the PC hardware platform for PC-based Automation from Siemens.

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

SIMOTION P320 is an Industrial PC for motion control.

Detailed information about the vulnerability is provided below.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (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 Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Mitigating Factors

Affected are devices with Intel Core i5, Intel Core i7 or Intel XEON.

## SOLUTION

Siemens provides firmware updates for the affected Industrial PCs [2].

As a general security measure Siemens strongly recommends to protect network access to the non-perimeter Industrial Products with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the products in a protected IT environment.

## ADDITIONAL RESOURCES

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

[2] https://support.industry.siemens.com/cs/ww/en/view/109747626

[3] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[4] Information about Industrial Security by Siemens: https://www.siemens.com/industrialsecurity

[5] For further inquiries on 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

## DISCLAIMER