

SSA-892715: ME, SPS and TXE Vulnerabilities in SIMATIC IPCs

Publication Date: 2018-02-22
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 8.2

SUMMARY

Intel has identified vulnerabilities in Intel Management Engine (ME), Intel Server Platform Services (SPS), and Intel Trusted Execution Engine (TXE). As several Siemens Industrial PCs use Intel technology, they are also affected.

Siemens has released updates for the affected Industrial PCs.

AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|--|---|
| SIMATIC Field-PG M3: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48791866 |
| SIMATIC Field-PG M4: BIOS < V18.01.06 | Update to V18.01.06 or higher https://support.industry.siemens.com/cs/ww/en/view/109037537 |
| SIMATIC Field-PG M5: BIOS < V22.01.04 | Update to V22.01.04 or higher https://support.industry.siemens.com/cs/ww/en/view/109738122 |
| SIMATIC HMI IPC677C: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |
| SIMATIC IPC427D (incl. SIPLUS variants): BIOS < V17.0?.10 | Update to V17.0?.10 or higher https://support.industry.siemens.com/cs/ww/en/view/108608500 |
| SIMATIC IPC427E (incl. SIPLUS variants): BIOS < V21.01.07 | Update to V21.01.07 or higher https://support.industry.siemens.com/cs/ww/en/view/109742593 |
| SIMATIC IPC477D: BIOS < V17.0?.10 | Update to V17.0?.10 or higher https://support.industry.siemens.com/cs/ww/en/view/108608500 |
| SIMATIC IPC477D PRO: BIOS < V17.0?.10 | Update to V17.0?.10 or higher https://support.industry.siemens.com/cs/ww/en/view/108608500 |
| SIMATIC IPC477E: BIOS < V21.01.07 | Update to V21.01.07 or higher https://support.industry.siemens.com/cs/ww/en/view/109742593 |
| SIMATIC IPC547D: ME < V7.1.91.3272 | Update to V7.1.91.3272 or higher https://support.industry.siemens.com/cs/ww/en/view/67329515 |

| | |
|---|--|
| SIMATIC IPC547E: ME < V9.1.41.3024 | Update to V9.1.41.3024 or higher https://support.industry.siemens.com/cs/ww/en/view/109481624 |
| SIMATIC IPC547G: ME < V11.8.50.3425 and BIOS < R1.21.0 | Update to V11.8.50.3425 and R1.21.0 or higher https://support.industry.siemens.com/cs/ww/en/view/109750349 |
| SIMATIC IPC627C: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |
| SIMATIC IPC627D: ME < V9.1.41.3024 | Update to V9.1.41.3024 or higher https://support.industry.siemens.com/cs/ww/en/view/109474954 |
| SIMATIC IPC647C: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792076 |
| SIMATIC IPC647D: ME < V9.1.41.3024 | Update to V9.1.41.3024 or higher https://support.industry.siemens.com/cs/ww/en/view/109037779 |
| SIMATIC IPC677D: ME < V9.1.41.3024 | Intall V9.1.41.3024 or higher https://support.industry.siemens.com/cs/ww/en/view/109474954 |
| SIMATIC IPC827C: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |
| SIMATIC IPC827D: ME < V9.1.41.3024 | Update to V9.1.41.3024 or higher https://support.industry.siemens.com/cs/ww/en/view/109474954 |
| SIMATIC IPC847C: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792076 |
| SIMATIC IPC847D: ME < V9.1.41.3024 | Update to V9.1.41.3024 or higher https://support.industry.siemens.com/cs/ww/en/view/109037779 |
| SIMATIC ITP1000: BIOS < V23.01.03 | Update to V23.01.03 or higher https://support.industry.siemens.com/cs/ww/en/view/109748173 |
| SIMOTION P320-4S: BIOS < S17.02.06.83.1 | Update to S17.02.06.83.1 or higher https://support.industry.siemens.com/cs/ww/en/view/109756438 |
| SINUMERIK PCU50.5-C, WIN7: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |
| SINUMERIK PCU50.5-C, WINXP: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |
| SINUMERIK PCU50.5-P, WIN7: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |

| | |
|--|---|
| SINUMERIK PCU50.5-P, WINXP: ME < V6.2.61.3535 | Update to V6.2.61.3535 or higher https://support.industry.siemens.com/cs/ww/en/view/48792087 |
|--|---|

WORKAROUNDS AND MITIGATIONS

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

- The attacker must have network access for CVE-2017-5712 and local access for all other vulnerabilities. Siemens recommends operating the devices only within trusted networks.

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.

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

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-2017-5705

Multiple buffer overflows could allow attackers to execute arbitrary code. Local access to the system is required to exploit this vulnerability.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 8.2 |
| CVSS Vector | 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 |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

Vulnerability CVE-2017-5706

Multiple buffer overflows could allow attackers to execute arbitrary code. Local access to the system is required to exploit this vulnerability.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 8.2 |
| CVSS Vector | 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 |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

Vulnerability CVE-2017-5707

Multiple buffer overflows could allow attackers to execute arbitrary code. Local access to the system is required to exploit this vulnerability.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 8.2 |
| CVSS Vector | 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 |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

Vulnerability CVE-2017-5708

Multiple privilege escalations could allow unauthenticated access to sensitive data.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C |
| CWE | CWE-264: Permissions, Privileges, and Access Controls |

Vulnerability CVE-2017-5709

Multiple privilege escalations could allow unauthenticated access to sensitive data.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C |
| CWE | CWE-264: Permissions, Privileges, and Access Controls |

Vulnerability CVE-2017-5710

Multiple privilege escalations could allow unauthenticated access to sensitive data.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C |
| CWE | CWE-264: Permissions, Privileges, and Access Controls |

Vulnerability CVE-2017-5711

Multiple buffer overflows could allow attackers with local access to execute arbitrary code.

| | |
|----------------------|--|
| 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:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

Vulnerability CVE-2017-5712

A buffer overflow could allow remote authenticated attackers to execute arbitrary code with extended privileges.

| | |
|----------------------|--|
| CVSS v3.1 Base Score | 7.2 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

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

ADDITIONAL INFORMATION

Further information can be found on <https://support.industry.siemens.com/cs/ww/de/view/109747626>. Information from Intel can be found on <https://www.intel.com/content/www/us/en/support/articles/000025619/software.html>.

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 (2018-02-22): | Publication Date |
| V1.1 (2018-04-18): | Updated SIOS links |
| V1.2 (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.