SSA-377318: Multiple vulnerabilities in Intel Active Management Technology (AMT) of SIMATIC IPCs

Publication Date: 2019-02-12
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 6.7

SUMMARY

There are multiple vulnerabilities in the Intel Management Engine used in multiple SIMATIC IPC devices that may allow arbitrary code execution, a partial denial of service or information disclosure. For additional information see: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00141.html.

Siemens provides updates for the affected devices.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC FieldPG M5: All versions < V22.01.06	Update to V22.01.06 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC427E (incl. SIPLUS variants): All versions < V21.01.09	Update to V21.01.09 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC477E: All versions < V21.01.09	Update to V21.01.09 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC547E: All versions < R1.30.0	Update to R1.30.0 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC547G: All versions < R1.23.0	Update to R1.23.0 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC627D: All versions < V19.02.11	Update to V19.02.11 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC647D: All versions < V19.01.14	Update to V19.01.14 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC677D: All versions < V19.02.11	Update to V19.02.11 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC IPC827D: All versions < V19.02.11	Update to V19.02.11 https://support.industry.siemens.com/cs/us/en/view/109747626

SIMATIC IPC847D: All versions < V19.01.14	Update to V19.01.14 https://support.industry.siemens.com/cs/us/en/view/109747626
SIMATIC ITP1000: All versions < V23.01.04	Update to V23.01.04 https://support.industry.siemens.com/cs/us/en/view/109747626

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 malicious code on affected systems. Therefore, Siemens recommends determining if it is possible that untrusted code can be run on these systems, or if existing measures implemented by the operator reduce the likelihood of untrusted code being run.

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, SIMATIC FieldPGs and SIMATIC ITPs are the PC hardware platforms 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.

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-2018-3616

Bleichenbacher-style side channel vulnerability in TLS implementation in Intel Active Management Technology before 12.0.5 may allow an unauthenticated user to potentially obtain the TLS session key via the network.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality of the device.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2018-3657

Multiple buffer overflows in Intel AMT in Intel CSME firmware versions before version 12.0.5 may allow a privileged user to potentially execute arbitrary code with Intel AMT execution privilege via local access.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the device.

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-20: Improper Input Validation

Vulnerability CVE-2018-3658

Multiple memory leaks in Intel AMT in Intel CSME firmware versions before 12.0.5 may allow an unauthenticated user with Intel AMT provisioned to potentially cause a partial denial of service via network access.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-401: Improper Release of Memory Before Removing Last Reference (‘Memory Leak’)

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 (2019-02-12): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE