

SSA-113131: Denial of Service Vulnerabilities in SIMATIC S7-400 CPUs

Publication Date: 2018-11-13
 Last Update: 2023-05-09
 Current Version: V1.5
 CVSS v3.1 Base Score: 8.2

SUMMARY

Two vulnerabilities have been identified in the SIMATIC S7-400 CPU family that could allow an attacker to cause a denial of service condition. In order to exploit the vulnerabilities, an attacker must have access to the affected devices on port 102/tcp via Ethernet, PROFIBUS or Multi Point Interfaces (MPI).

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-400 CPU 412-1 DP V7 (6ES7412-1XJ07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 412-2 DP V7 (6ES7412-2XK07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414-2 DP V7 (6ES7414-2XL07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414-3 DP V7 (6ES7414-3XM07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416-2 DP V7 (6ES7416-2XP07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-400 CPU 416-3 DP V7 (6ES7416-3XS07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416F-2 DP V7 (6ES7416-2FP07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 417-4 DP V7 (6ES7417-4XT07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 412-2 PN V7 (6ES7412-2EK07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V4.5 and below CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.9	Update to V6.0.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109474550/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-410 CPU family (incl. SIPLUS variants): All versions < V8.2.1	Update to V8.2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109476571/ Activate Field Interface Security in PCS 7 V9.0, and use a SIMATIC/SIPLUS CP443-1 Adv. to communicate with ES/OS See further recommendations from section Workarounds and Mitigations
SIPLUS S7-400 CPU 414-3 PN/DP V7 (6AG1414-3EM07-7AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations

SIPLUS S7-400 CPU 416-3 PN/DP V7 (6AG1416-3ES07-7AB0): All versions < V7.0.3	Update to V7.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109752685/ See recommendations from section Workarounds and Mitigations
SIPLUS S7-400 CPU 416-3 V7 (6AG1416-3XS07-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-400 CPU 417-4 V7 (6AG1417-4XT07-7AB0): All versions	Currently no fix is planned See 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:

- CVE-2018-16557: Configure protection level 3 (read/write protection)
- Restrict network access to affected devices; restrict network access to port 102/tcp for Ethernet interfaces

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 S7-400 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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-2018-16556

Specially crafted packets sent to port 102/tcp via Ethernet interface, via PROFIBUS, or via Multi Point Interfaces (MPI) could cause the affected devices to go into defect mode. Manual reboot is required to resume normal operation.

Successful exploitation requires an attacker to be able to send specially crafted packets to port 102/tcp via Ethernet interface, via PROFIBUS or Multi Point Interfaces (MPI). No user interaction and no user privileges are required to exploit the security vulnerability. The vulnerability could allow causing a denial of service condition of the core functionality of the CPU, compromising the availability of the system.

CVSS v3.1 Base Score 7.5
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2018-16557

Sending of specially crafted packets to port 102/tcp via Ethernet interface via PROFIBUS or Multi Point Interfaces (MPI) could cause a denial of service condition on affected devices. Flashing with a firmware image may be required to recover the CPU.

Successful exploitation requires an attacker to have network access to port 102/tcp via Ethernet interface or to be able to send messages via PROFIBUS or Multi Point Interfaces (MPI) to the device. No user interaction is required. If no access protection is configured, no privileges are required to exploit the security vulnerability. The vulnerability could allow causing a denial of service condition of the core functionality of the CPU, compromising the availability of the system.

CVSS v3.1 Base Score 8.2
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C](#)
CWE CWE-347: Improper Verification of Cryptographic Signature

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned
- Zhang JiaWei and Qing YuLong from CNCERT/CC for coordinated disclosure of vulnerability CVE-2018-16556

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 (2018-11-13): Publication Date
V1.1 (2019-05-14): Updated acknowledgements and added solution for S7-400H V6
V1.2 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products
V1.3 (2022-08-09): No fix planned for SIMATIC S7-400 PN/DP V6 and below CPU family, and for SIMATIC S7-400 H V4.5 and below CPU family
V1.4 (2023-01-10): No fix planned for SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)
V1.5 (2023-05-09): Expanded SIMATIC S7-400 V7 CPU family (incl. SIPLUS variants) to individual products and MLFBs; added fix for SIMATIC S7-400 PN/DP V7 CPUs; clarified that no fix is planned for other S7-400 V7 CPUs

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.