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

Publication Date: 2018-11-13
Last Update: 2020-02-10
Current Version: V1.2
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 vulnerability, an attacker must have access to the affected devices on port 102/tcp via Ethernet, PROFIBUS or Multi Point Interfaces (MPI).

Siemens provides updates to address the vulnerability, and recommends specific mitigations.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-400 DP V7 CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V4.5 and below CPU family (incl. SIPLUS variants): All versions	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 https://support.industry.siemens.com/cs/ww/en/view/109474550
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	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 https://support.industry.siemens.com/cs/ww/en/view/109476571

WORKAROUNDS AND MITIGATIONS

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

- Configure protection level 3 (read/write protection) to mitigate CVE-2018-16557
- Restrict network access to affected devices; restrict network access to port 102/tcp for Ethernet interfaces
- For SIMATIC/SIPLUS S7-CPU 410 CPUs: Activate Field Interface Security in PCS 7 V9.0, and use a SIMATIC/SIPLUS CP443-1 Adv. to communicate with ES/OS
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

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

Products in the SIMATIC S7-400 CPU family have been designed for process control in industrial environments. They are used worldwide, e.g. in the automotive industry, mechanical equipment manufacture, warehousing systems, building engineering, steel industry, power generation and distribution, pharmaceuticals, food and beverages industry, or chemical industry.

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.

At the time of advisory publication no public exploitation of this security vulnerability was known.

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-730: OWASP Top Ten 2004 Category A9 - Denial of Service

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.

At the time of advisory publication no public exploitation of this security vulnerability was known.

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:

- Zhang JiaWei and Qing YuLong from CNCERT/CC for coordinated disclosure of vulnerability CVE-2018-16556
- 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 (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

TERMS OF USE