SSA-914382: Denial-of-Service Vulnerability in SIMATIC S7-400 CPU Family

Publication Date: 2018-05-15
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

SIMATIC S7-400 CPUs are affected by a security vulnerability which could lead to a Denial-of-Service condition of the PLC if specially crafted packets are received and processed.

The affected SIMATIC S7-400 CPU hardware versions are in the product cancellation phase or already phased-out. Siemens recommends customers either upgrading to a new version or implementing specific countermeasures.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-400 CPU hardware version 4.0 and below (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations or upgrade to hardware version 5.0 or newer https://support.industry.siemens.com/cs/ww/en/view/109483507
SIMATIC S7-400 CPU hardware version 5.0 (incl. SIPLUS variants): All firmware versions < V5.2	Update to firmware version 5.2 or newer https://support.industry.siemens.com/cs/ww/en/view/109474827
SIMATIC S7-400 H CPU hardware version 4.5 and below (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations or upgrade to hardware version 6.0 or newer https://support.industry.siemens.com/cs/ww/en/view/75407031

WORKAROUNDS AND MITIGATIONS

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

- Apply cell protection concept: https://www.siemens.com/cert/operational-guidelines-industrial-security.
- Use VPN for protecting network communication between cells.
- 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-2018-4850

The affected CPUs improperly validate S7 communication packets which could cause a Denial-of-Service condition of the CPU. The CPU will remain in DEFECT mode until manual restart.

Successful exploitation requires an attacker to be able to send a specially crafted S7 communication packet to a communication interface of the CPU. This includes Ethernet, PROFIBUS, and Multi Point Interfaces (MPI). No user interaction or 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. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.

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

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 (2018-05-15): Publication Date
V1.1 (2018-09-11): Added hint to Workarounds section
V1.2 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE