SSA-557541: Denial-of-Service Vulnerability in SIMATIC S7-400 CPUs

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

SIMATIC S7-400 CPU devices contain an input validation vulnerability that could allow an attacker to create a Denial-of-Service condition. A restart is needed to restore normal operations.

Siemens has released an update for SIMATIC S7-410 V10 CPU family and SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants for both) and recommends to update to the latest version. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.10	Update to V6.0.10 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 V7 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants): All versions < V10.1	Update to V10.1 or later version To obtain SIMATIC S7-410 V10.1 contact your local support. See further 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:

- Limit access to port 102/tcp to trusted users and systems only

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

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-2021-40368

Affected devices improperly handle specially crafted packets sent to port 102/tcp.

This could allow an attacker to create a Denial-of-Service condition. A restart is needed to restore normal operations.

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

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 (2022-04-12): Publication Date

TERMS OF USE