SSA-431678: Denial-of-Service Vulnerability in SIMATIC S7 CPU Families

Publication Date: 2020-02-11
Last Update: 2020-04-14
Current Version: V1.2
CVSS v3.1 Base Score: 5.3

SUMMARY

SIMATIC S7 CPU families are affected by a vulnerability that could allow remote attackers to perform a Denial-of-Service attack by sending a specially crafted HTTP request to the web server of an affected device.

Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.1	Update to V4.1 or any later version https://support.industry.siemens.com/cs/ww/en/view/109763919
SIMATIC S7-300 PN/DP CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.17	Update to V3.X.17 https://support.industry.siemens.com/cs/ww/en/ps/13752/dl
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX (F) 2010: All versions	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:

- Restrict access to the device to the internal or VPN network. Further, if possible, restrict access to the web server (80/tcp, 443/tcp) to trusted IP addresses.
- If possible in your environment, disable the integrated web server. The web server is disabled in the default settings and its use is optional.

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

Siemens SIMATIC S7-300 CPU families, S7-400 CPU families and S7-1200 CPU families 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.

SIMATIC WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

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-2019-13940

Affected devices contain a vulnerability that could cause a Denial-of-Service condition of the web server by sending specially crafted HTTP requests to ports 80/tcp and 443/tcp.

The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device's web server. Beyond the web service, no other functions or interfaces are affected by the Denial-of-Service condition.

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-400: Uncontrolled Resource Consumption

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 (2020-02-11):	Publication Date
V1.1 (2020-03-10):	Updated solution for SIMATIC S7-300 PN/DP CPU family
V1.2 (2020-04-14):	Added SIMATIC WinAC RTX to the list of affected products

TERMS OF USE