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

Publication Date: 2020-02-11
Last Update: 2023-01-10
Current Version: V1.4
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 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 ET 200pro IM154-8 PN/DP CPU (6ES7154-8AB01-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47354502/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8F PN/DP CPU (6ES7154-8FB01-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47354578/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200pro IM154-8FX PN/DP CPU (6ES7154-8FX00-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/62612377/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM151-8 PN/DP CPU (6ES7151-8AB01-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200S IM151-8F PN/DP CPU (6ES7151-8FB01-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations

SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FJ14-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 315T-3 PN/DP (6ES7315-7TJ10-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/85049260/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317-2 PN/DP (6ES7317-2EK14-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317F-2 PN/DP (6ES7317-2FK14-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317T-3 PN/DP (6ES7317-7TK10-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/85059804/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 317TF-3 PN/DP (6ES7317-7UL10-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/85063017/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 319-3 PN/DP (6ES7318-3EL01-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/44442927/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU 319F-3 PN/DP (6ES7318-3FL01-0AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/44443101/ 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 S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.1	Update to V4.1 or later version https://support.industry.siemens.com/cs/ww/en/view/106200276/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX 2010 (6ES7671-0RC08-0YA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX F 2010 (6ES7671-1RC08-0YA0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM151-8 PN/DP CPU (6AG1151-8AB01-7AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47353723/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200S IM151-8F PN/DP CPU (6AG1151-8FB01-2AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/47354354/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 314C-2 PN/DP (6AG1314-6EH04-7AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/51466769/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315-2 PN/DP (6AG1315-2EH14-7AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40360647/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 315F-2 PN/DP (6AG1315-2FJ14-2AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40944925/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317-2 PN/DP (6AG1317-2EK14-7AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40362228/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-300 CPU 317F-2 PN/DP (6AG1317-2FK14-2AB0): All versions < V3.X.17	Update to V3.X.17 or later version https://support.industry.siemens.com/cs/ww/en/view/40945128/ 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:

- Restrict access to the device to the internal or VPN network and to trusted IP addresses only
- Disable the web server. Note that this feature is disabled by default
- Restrict access to the web server (80/tcp, 443/tcp) to trusted IP addresses

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 S7-300, S7-400 and and S7-1200 CPU controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

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-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.

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
V1.3 (2022-08-09):	No fix planned for SIMATIC S7-400 PN/DP V6 and below CPU family
V1.4 (2023-01-10):	No fix planned for remaining products. SIMATIC S7-300 CPU family expanded with product specific designations, patch links and MLFBs

TERMS OF USE