SSA-382653: Multiple Denial of Service Vulnerabilities in Industrial Products

Publication Date:	2022-12-13
Last Update:	2022-12-13
Current Version:	V1.0
CVSS v3.1 Base Score:	7.5

SUMMARY

Affected SIMATIC firmware contains multiple vulnerabilities that could allow an unauthenticated attacker to perform a denial-of-service attack under certain conditions.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller family: All versions < V3.0.1	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.6.0	Update to V4.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814248/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.0.1	Update to V3.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V5.0	Update to V5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109809300/ See further recommendations from section Workarounds and Mitigations
SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

TIM 1531 IRC (6GK7543-1MX00-0XE0): All versions	Currently no fix is available 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 port 102/tcp to trusted systems e.g. with an external firewall

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 Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

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

SIMATIC S7-1500 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

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.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2021-40365

Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

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

Vulnerability CVE-2021-44693

Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-1284: Improper Validation of Specified Quantity in Input

Vulnerability CVE-2021-44694

Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-1287: Improper Validation of Specified Type of Input

Vulnerability CVE-2021-44695

Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-1286: Improper Validation of Syntactic Correctness of Input

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Gao Jian for coordinated disclosure

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 (2022-12-13): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.