SSA-693975: Denial-of-Service Vulnerability in the Web Server of Industrial Products

Publication Date: 2023-12-12
Last Update: 2024-03-12
Current Version: V1.1
CVSS v3.1 Base Score: 7.5
CVSS v4.0 Base Score: 8.7

SUMMARY

A vulnerability in the affected products could allow an unauthorized attacker with network access to the webserver of an affected device to perform a denial-of-service attack.

Siemens has released a new version for SINAMICS S210 (6SL5...) and recommends to update to the latest version. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 1242-7 V2 (incl. SIPLUS variants): All versions < V3.4.29 affected by all CVEs	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (incl. SIPLUS variants): All versions < V3.4.29 affected by all CVEs	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 IEC (incl. SIPLUS variants): All versions < V3.4.29 affected by all CVEs	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE: All versions < V3.4.29 affected by all CVEs	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/ See further recommendations from section Workarounds and Mitigations

SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions < V3.4.29 affected by all CVEs	Update to V3.4.29 or later version https://support.industry.siemens.com/cs/ww/en/view/109823721/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions < V3.0.37 affected by all CVEs	Update to V3.0.37 or later version https://support.industry.siemens.com/cs/ww/en/view/109828349/ See further recommendations from section Workarounds and Mitigations
SINAMICS S210 (6SL5...): All versions >= V6.1 < V6.1 HF2 affected by all CVEs	Update to V6.1 HF2 or later version https://support.industry.siemens.com/cs/ww/en/view/109825153/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions < V3.0.37 affected by all CVEs	Update to V3.0.37 or later version https://support.industry.siemens.com/cs/ww/en/view/109828349/ 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 network access to the integrated webserver

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 CP 1242 and CP 1243 related processors connect SIMATIC S7-1200 controllers to Wide Area Networks (WAN). They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 1543-1 communications processors connect SIMATIC S7-1500 controllers to Ethernet networks. They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

With the SINAMICS converter series you can solve drive tasks in the low, medium and DC voltage range.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-38380

The webserver implementation of the affected products does not correctly release allocated memory after it has been used.

An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-401: Missing Release of Memory after Effective Lifetime

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 (2023-12-12):	Publication Date
V1.1 (2024-03-12):	Added fixes for supported SIMATIC S7-1200 CP 1200 family, added fix version for SIMATIC CP1200 family and SIMATIC CP1500 family

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.