SSA-517377: Multiple Vulnerabilities in the SRCS VPN Feature in SIMATIC CP Devices

Publication Date: 2022-07-12
Last Update: 2023-03-14
Current Version: V1.2
CVSS v3.1 Base Score: 10.0

SUMMARY

The below referenced devices contain multiple vulnerabilities that could be exploited when the SINEMA Remote Connect Server (SRCS) VPN feature is used. The feature is not activated by default. The most severe could allow an attacker to execute arbitrary code with elevated privileges under certain circumstances.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations

SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions < V3.0.22	Update to V3.0.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions >= V2.0 < V2.2.28	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions < V3.0.22	Update to V3.0.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678/ See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 See further recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218 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:

- Block access to port 5243/udp e.g. with an external firewall if possible
- Disable the SINEMA Remote Connect Server (SRCS) VPN feature

- Make sure to configure the CP to only connect to trusted SINEMA Remote Connect Server instances

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 1242-7 and CP 1243-7 LTE communications 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 1243-8 IRC communications processors connect SIMATIC S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

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.

SIMATIC CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communications processors connect SIMATIC ET 200SP controllers to Ethernet networks. SIMATIC CP 1543SP-1 and CP 1542SP-1 IRC communications processors also provide integrated security functions such as firewall, Virtual Private Networks (VPN) or support other protocols with data encryption.

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-2022-34819

The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2022-34820

The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2022-34821

By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')

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 (2022-07-12):	Publication Date
V1.1 (2022-08-09):	Added fix for SIMATIC CP 1242-7 V2, CP 1243-7, CP 1243-1, CP 1243-8
V1.2 (2023-03-14):	Added fix for SIMATIC CP 1542SP-1 IRC, and SIMATIC CP 1543SP-1

TERMS OF USE