SSA-539476: Siemens SIMATIC NET CP, SINEMA and SCALANCE Products Affected by Vulnerabilities in Third-Party Component strongSwan

Publication Date:	2022-02-08
Last Update:	2023-03-14
Current Version:	V1.4
CVSS v3.1 Base Score:	7.5

SUMMARY

Vulnerabilities in the third-party component strongSwan could allow an attacker to cause a denial of service (DoS) condition in affected devices by exploiting integer overflow bugs.

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
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/

SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions < V7.1	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V2.3 only affected by CVE-2021-41991	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V2.3 only affected by CVE-2021-41991	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/

SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V2.3 only affected by CVE-2021-41991	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V2.3 only affected by CVE-2021-41991	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V2.3 only affected by CVE-2021-41991	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109805907/
SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/ Only deploy certificates via TIA portal that got created with TIA portal

SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V3.0.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678/ Only deploy certificates via TIA portal that got created with TIA portal
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0): All versions < V1.1 only affected by CVE-2021-41991	Update to V1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811116/ Only deploy certificates via TIA portal that got created with TIA portal
SINEMA Remote Connect Server: All versions < V3.1 only affected by CVE-2021-41991	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811169/
SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions < V2.2.28 only affected by CVE-2021-41991	Update to V2.2.28 or later version https://support.industry.siemens.com/cs/ww/en/view/109817067/
SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions < V3.0.22 only affected by CVE-2021-41991	Update to V3.0.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678/ Only deploy certificates via TIA portal that got created with TIA portal

SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions < V3.3.46 only affected by CVE-2021-41991	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218/ Only deploy certificates via TIA portal that got created with TIA portal

WORKAROUNDS AND MITIGATIONS

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

RUGGEDCOM RM1224 is a 4G ROUTER for wireless IP-communication from Ethernet based devices via LTE(4G)- mobile radio.

SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 are industrial routers.

SCALANCE SC-600 devices (SC622-2C, SC626-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

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 1243-1 communications processors connect S7-1200 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 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC 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 1545-1 communications processors connect the 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.

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

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-2021-41990

The gmp plugin in strongSwan before version 5.9.4 has a remote integer overflow vulnerability via a crafted certificate with an RSASSA-PSS signature. For example, this can be triggered by an unrelated self-signed CA certificate sent by an initiator. Remote code execution cannot occur.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-41991

The in-memory certificate cache in strongSwan before version 5.9.4 has a remote integer overflow vulnerability upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator, but this is not done correctly. This could lead to a denial of service (DoS) condition. Remote code execution can't be excluded completely, but it would require attackers to have control over the dereferenced memory, so it is very unlikely.

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-190: Integer Overflow or Wraparound

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 (2022-02-08):	Publication Date
V1.1 (2022-04-12):	Added solutions for SCALANCE S615, SCALANCE M-800 Family, SCALANCE MUM-800 Family, RUGGEDCOM RM1224 family, SIMATIC CP 1543-1, and SIPLUS NET CP 1543-1
V1.2 (2022-06-14):	Added fix for SIMATIC CP 1545-1 and SINEMA Remote Connect Server
V1.3 (2022-08-09):	Added fix for SIMATIC CP 1242-7 V2, CP 1243-7, CP 1243-1, CP 1243-8
V1.4 (2023-03-14):	Added fix for SIMATIC CP 1542SP-1, SIMATIC CP 1542SP-1 IRC, and SIMATIC CP 1543SP-1

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.