SSA-712929: Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industrial Products

Publication Date: 2022-06-14
Last Update: 2022-06-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability in the openSSL component (CVE-2022-0778, [0]) could allow an attacker to create a denial of service condition by providing specially crafted elliptic curve certificates to products that use a vulnerable version of openSSL.

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.

[0] https://www.openssl.org/news/secadv/20220315.txt

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Industrial Edge - OPC UA Connector: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
Industrial Edge - PROFINET IO Connector: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
Industrial Edge - SIMATIC S7 Connector App: All versions < V1.7.0	Use the Edge Management System to update to V1.7.0 or later version https://www.siemens.com/industrial-edge-marketplace/
RUGGEDCOM CROSSBOW Station Access Controller: All versions only running on ROX	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX MX5000RE: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

RUGGEDCOM ROX RX1400: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1500: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1501: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1510: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1511: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1512: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1524: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX1536: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
RUGGEDCOM ROX RX5000: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE LPE9403 (6GK5998-3GS00-2AC2): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109811123/
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM853-1 (RoW) (6GK5853-2EA00-2AA1): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (NAM) (6GK5856-2EA00-3BA1): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V2.3.1	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/

SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V2.3.1	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V2.3.1	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V2.3.1	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V2.3.1	Update to V2.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109810992/
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Advanced (6GK7343-1GX31-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1626 (6GK1162-6AA01): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 1628 (6GK1162-8AA00): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC Logon: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC MV540 H (6GF3540-0GE10): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC MV540 S (6GF3540-0CD10): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC MV550 H (6GF3550-0GE10): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC MV550 S (6GF3550-0CD10): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC MV560 U (6GF3560-0LE10): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC MV560 X (6GF3560-0HE10): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V14: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIMATIC NET PC Software V15: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V16: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V17: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 TeleControl: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC PDM: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC RF166C (6GT2002-0EE20): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF185C (6GT2002-0JE10): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF186C (6GT2002-0JE20): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF186CI (6GT2002-0JE50): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF188C (6GT2002-0JE40): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF188CI (6GT2002-0JE60): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811120/
SIMATIC RF360R (6GT2801-5BA30): All versions < V2.0.1	Update to V2.0.1 or later version https://support.industry.siemens.com/cs/de/en/view/109811118/
SIMATIC RF610R (6GT2811-6BC10): All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF615R (6GT2811-6CC10): All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF650R (6GT2811-6AB20): All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/

SIMATIC RF680R (6GT2811-6AA10): All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC RF685R (6GT2811-6CA10): All versions < V4.0.1	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811014/
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller (incl. F): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V5.X: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAUT Software ST7sc: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINAUT ST7CC: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINEC INS: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINEC NMS: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SINEMA Remote Connect Server: All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811169/
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 Advanced (6AG1343-1GX31-4XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions	Currently no fix is available See 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
TeleControl Server Basic V3: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
TIA Administrator: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
TIA Portal Cloud: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
TIA Portal V15: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
TIA Portal V16: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
TIA Portal V17: 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

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

Industrial Edge represents an open, ready-to-use Edge computing platform consisting of Edge devices, Edge apps, Edge connectivity, and an application and device management infrastructure.

SCALANCE LPE9000 (Local Processing Engine) extends the SCALANCE family portfolio by a component that provides computing power for a wide range of applications in the network, close to the process – Edge Computing.

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

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.

The SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

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-2022-0778

The BN_mod_sqrt() function in openSSL, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. (https://www.openssl.org/news/secadv/20220315.txt)

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-835: Loop with Unreachable Exit Condition (‘Infinite Loop’)

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 (2022-06-14): 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.