SSA-772220: OpenSSL Vulnerabilities in Industrial Products

Publication Date: 2021-07-13
Last Update: 2024-01-09
Current Version: V2.3
CVSS v3.1 Base Score: 5.9

SUMMARY

OpenSSL has published a security advisory [0] about a vulnerability in OpenSSL versions 1.1.1 < 1.1.1k, that allows an unauthenticated attacker to cause a Denial-of-Service (DoS) if a maliciously crafted renegotiation message is sent.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where fixes are not, or not yet available.

[0] https://www.openssl.org/news/secadv/20210325.txt

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM CROSSBOW Station Access Controller (SAC): All versions >= V5.2.0 < V5.3 only when running on ROX II V2.14.0	Update to V5.3 or later version Update ROX II to V2.14.1 (https://support.industry.siemens.com/cs/ww/en/view/109800780/) or later version https://support.industry.siemens.com/cs/ww/en/view/109813558/
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276/
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276/
SCALANCE LPE9403 (6GK5998-3GS00-2AC2): All versions < V1.1	Update to V1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109805118/
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276

SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions >= V6.2 < V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE S602: All versions >= V4.1	Currently no fix is planned

SCALANCE S612: All versions >= V4.1	Currently no fix is planned
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions >= V6.2 <V7.1	Update to V7.1 or later version use TLS v1.3 only https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE S623: All versions >= V4.1	Currently no fix is planned
SCALANCE S627-2M: All versions >= V4.1	Currently no fix is planned
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions >= V2.0 < V2.1.4	Update to V2.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109797244
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions >= V2.0 < V2.1.4	Update to V2.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109797244
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions >= V2.0 < V2.1.4	Update to V2.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109797244
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions >= V2.0 < V2.1.4	Update to V2.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109797244
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions >= V2.0 < V2.1.4	Update to V2.1.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109797244
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions >= V2.0 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions >= V2.0 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions >= V2.0 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions >= V2.0 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/

SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions >= V2.0 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions >= V2.0 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/
SCALANCE W-700 IEEE 802.11n family: All versions >= V6.5	Currently no fix is planned
SCALANCE XB-200: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569
SCALANCE XC-200: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569
SCALANCE XF-200BA: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569
SCALANCE XM-400: All versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109796319
SCALANCE XP-200: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569
SCALANCE XR-300WG: All versions < V4.3	Update to V4.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109799569
SCALANCE XR-500 Family: All versions < V6.4	Update to V6.4 or later version https://support.industry.siemens.com/cs/ww/en/view/109796317
SIMATIC Cloud Connect 7 CC712 (6GK1411-1AC00): All versions >= V1.1 < V1.6	Update to V1.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109803418/
SIMATIC Cloud Connect 7 CC716 (6GK1411-5AC00): All versions >= V1.1 < V1.6	Update to V1.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109803418/
SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218

SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218
SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0): All versions >= V2.1 < V2.2.28	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 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109800773
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions >= V2.1 < V2.2.28	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 >= V1.0 < V1.1	Update to V1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811116/
SIMATIC HMI Comfort Outdoor Panels (incl. SIPLUS variants): All versions < V17.0 Upd 2	Update to V17.0 Upd 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SIMATIC HMI Comfort Panels (incl. SIPLUS variants): All versions < V17.0 Upd 2	Update to V17.0 Upd 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SIMATIC HMI KTP Mobile Panels: All versions < V17.0 Upd 2	Update to V17.0 Upd 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SIMATIC Logon V1.6: All versions >= V1.6 Upd2 < V1.6 Upd5	Update to V1.6 Upd5 or later version Restrict access to Remote Access service, if used, to mitigate this issue. This service is disabled by default. https://support.industry.siemens.com/cs/ww/en/view/109794407/

SIMATIC MV540 H (6GF3540-0GE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109804366
SIMATIC MV540 S (6GF3540-0CD10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109804366
SIMATIC MV550 H (6GF3550-0GE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109804366
SIMATIC MV550 S (6GF3550-0CD10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109804366
SIMATIC MV560 U (6GF3560-0LE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109804366
SIMATIC MV560 X (6GF3560-0HE10): All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109804366
SIMATIC PCS 7 TeleControl: All versions < V9.1	Update to V9.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109805072/
SIMATIC PCS neo: All versions < V3.1	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109801424/
SIMATIC PDM: All versions >= V9.1 SP7 < V9.2 SP1	Update to V9.2 SP 1 or later version Restrict access to the command interface, if used, to mitigate this issue. This interface is disabled by default. https://support.industry.siemens.com/cs/ww/en/view/109805353/
SIMATIC Process Historian OPC UA Server: All versions >= 2019 < 2020 Upd1	Update SIMATIC PCS neo to V3.1 or later version To obtain SIMATIC PCS neo V3.1 contact your local support.
SIMATIC RF166C (6GT2002-0EE20): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808633
SIMATIC RF185C (6GT2002-0JE10): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808633

SIMATIC RF186C (6GT2002-0JE20): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808633
SIMATIC RF186CI (6GT2002-0JE50): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808633
SIMATIC RF188C (6GT2002-0JE40): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808633
SIMATIC RF188CI (6GT2002-0JE60): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808633
SIMATIC RF360R (6GT2801-5BA30): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808759
SIMATIC RF610R (6GT2811-6BC10): All versions < V4.0	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808361
SIMATIC RF615R (6GT2811-6CC10): All versions < V4.0	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808361
SIMATIC RF650R (6GT2811-6AB20): All versions < V4.0	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808361
SIMATIC RF680R (6GT2811-6AA10): All versions < V4.0	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808361
SIMATIC RF685R (6GT2811-6CA10): All versions < V4.0	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808361
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.5.2	Update to V4.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109793280/
SIMATIC S7-1500 CPU 1518-4 PN/DP MFP family (incl. SIPLUS variant): All versions < V2.9.3	Update to V2.9.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459/

SIMATIC WinCC Runtime Advanced: All versions < V17 Update 1	Update to V17 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109800912
SIMATIC WinCC TeleControl: All versions < V7.5	Update to V7.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109814522/
SINAMICS Connect 300: All versions	Currently no fix is planned
SINEC NMS: All versions >= V1.0.1 < V1.0.2	Update to V1.0 SP2 https://support.industry.siemens.com/cs/ww/en/view/109797645/
SINEMA Server: All versions V14 < V14 SP3	Update to V14 SP3 or later version https://support.industry.siemens.com/cs/ww/en/view/109801374/
SINUMERIK OPC UA Server: All versions < V3.1 SP1	Update to V3.1 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109801292
SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0): All versions >= V2.1 < V2.2.28	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 >= V2.1 < V2.2.28	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 >= V2.1 < V2.2.28	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 >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions >= V2.2 < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109800773
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions >= V3.1 < V3.3.46	Update to V3.3.46 or later version https://support.industry.siemens.com/cs/ww/en/view/109812218

SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0): All versions >= V2.0 < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798331
TIA Administrator: All versions < V1.0 SP4	Update to V1.0 SP4 or later version https://support.industry.siemens.com/cs/ww/en/view/114358/
TIM 1531 IRC (6GK7543-1MX00-0XE0): All versions >= V2.0 < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798331

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

SIMATIC Process Historian is the long term archive system for SIMATIC PCS 7, SIMATIC WinCC and SIMATIC PCS neo. It stores process values, alarms and batch data of production plants in its database and offers historical process data to reporting and visualization applications.

SIMATIC RF600 Readers are used for the contactless identification of every kind of object, e.g. transport containers, pallets, production goods, or it can be generally used for recording goods in bulk.

RUGGEDCOM CROSSBOW is a secure access management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices.

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.

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

SCALANCE S-600 devices (S602, S612, S623, S627-2M) are used to protect trusted industrial networks from untrusted networks. The S-600 devices are superseded by the SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C), or the SCALANCE S615.

SCALANCE SC-600 devices are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

SCALANCE W-1700 products are wireless communication devices based on IEEE 802.11ac standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE W1750D is an Access Point that supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously.

SCALANCE W-700 products are wireless communication devices based on IEEE 802.11ax or 802.11n standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SIMATIC Cloud Connect 7 is an IoT Gateway to connect programmable logic controllers to cloud services and enables the connection of field devices with OPC UA server Interface as OPC UA clients.

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.

The SIMATIC CP 1543-1 and SIMATIC CP 1545-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

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.

The SIMATIC CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connect the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC Logon is used for central user administration and access control in other SIMATIC applications.

SIMATIC MV500 products are stationary optical readers, used to reliably capture printed, lasered, drilled, punched and dotpeen codes on a variety of different surfaces.

SIMATIC PCS 7 TeleControl is a server based software for the integration of outstations for monitoring and controlling highly remote plant units (referred to as RTUs, usually with a small or medium degree of automation) into the PCS 7 control system. This is carried out by means of telecontrol protocols over a WAN (Wide Area Network).

SIMATIC PCS neo is a distributed control system (DCS).

SIMATIC PDM (Process Device Manager) is an universal, manufacturer-independent tool for configuration, parameter assignment, commissioning, diagnostics and maintenance of intelligent process devices (actors, sensors) and automation components (remote I/Os, multiplexer, process control units, compact controller).

SIMATIC RF185C, RF186C/CI, and RF188C/CI are communication modules for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet and OPC UA.

The SIMATIC RF360R reader extends the SIMATIC RF300 RFID system by a compact reader with an integrated Industrial Ethernet interface.

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.

The SIMATIC S7-1500 MFP CPUs provide functionality of standard S7-1500 CPUs with the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in

C/C++ and an additional second independent runtime environment to execute C/C++ applications parallel to the STEP 7 program if required.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC TeleControl for WinCC is a server based software for the integration of outstations for monitoring and controlling highly remote plant units (referred to as RTUs, usually with a small or medium degree of automation) into the WinCC SCADA system. This is carried out by means of telecontrol protocols over a WAN (Wide Area Network).

SINAMICS CONNECT 300 is designed to acquire data through the USS port of the converter and synchronize the data to MindSphere, the Siemens Industrial Cloud Operating System. It is perfectly fit to connect MICROMASTER MM420/430/440 as well as SINAMICS V20 & G120 drives to Mindsphere.

SINEC INS (Infrastructure Network Services) is a web-based application that combines various network services in one tool. This simplifies installation and administration of all network services relevant for industrial networks.

SINEC PNI (Primary Network Initialization) is program for initializing Siemens network components and Siemens controllers. In addition network-specific parameters, necessary for commissioning SCALANCE and RUGGEDCOM devices can be set.

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 Server is a network monitoring and management software designed by Siemens for use in Industrial Ethernet networks.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production 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.

TIA Administrator is a web-based framework that can incorporate different function modules for administrative tasks, as well as functions for managing SIMATIC software and licenses.

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-2021-3449

An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

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 (2021-07-13):	Publication Date
V1.1 (2021-08-10):	Removed RUGGEDCOM CloudConnect APE/VPE as it is not affected, added solution for SIMATIC NET CP 1543-1
V1.2 (2021-09-14):	Added solution for SIMATIC S7-1500 CPU 1518-4 PN/DP MFP, SIMATIC PCS neo, SIMATIC Process Historian OPC UA Server, SINEMA Server, and TIA Administrator, removed SIMATIC HMI Basic Panels 2nd Generation as the product is not affected
V1.3 (2021-11-09):	Added solution for SCALANCE SC-600, SIMATIC WinCC Runtime Advanced, SIMATIC CP 1242-7 GPRS V2, SIMATIC CP 1243-7 LTE and SIMATIC Cloud Connect 7; split SCALANCE SC-600 into individual products; removed SINEC PNI as it is not affected
V1.4 (2021-12-14):	Added solution for SIMATIC MV500 family and SINUMERIK OPC UA Server
V1.5 (2022-01-11):	Added solution for SIMATIC HMI Panels, SIMATIC Logon and SIMATIC PDM, clarified that no remediation is planned for SCALANCE W-700 IEEE 802.11n family
V1.6 (2022-02-08):	Added solution for SCALANCE LPE9403; clarified that no remediation is planned for SCALANCE W-1700 IEEE 802.11ac family; added RUGGEDCOM CROSSBOW Station Access Controller as affected product ; fixed affected versions for SINEC NMS
V1.7 (2022-02-17):	Added solution for SIMATIC S7-1200 CPU family
V1.8 (2022-04-12):	No fix planned for SINAMICS Connect 300; Added solution for SCALANCE M-800 / S615 family, RUGGEDCOM RM1224, and SCALANCE W-1700 IEEE 802.11ac family; Added SIMATIC RF600R family
V1.9 (2022-05-10):	Added solution for SIMATIC READER RF1xxC family and SIMATIC Reader RF360R and SIMATIC PCS 7 TeleControl
V2.0 (2022-06-14):	Added fix for SIMATIC CP 1545-1
V2.1 (2022-08-09):	Added or corrected fix information for SIMATIC CP 1242-7 V2, CP 1243-7, CP 1243-1, CP 1243-8
V2.2 (2023-03-14):	Updated fix information for RUGGEDCOM CROSSBOW SAC, added fix for SIMATIC CP 1542SP-1 IRC, and SIMATIC CP 1543SP-1
V2.3 (2024-01-09):	Added fix for SIMATIC WinCC TeleControl

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.