# SSA-772220: OpenSSL Vulnerabilities in Industrial Products

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
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 is preparing updates and recommends countermeasures for products where updates 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 CloudConnect APE/VPE:<br>All versions | See recommendations from section Workarounds and Mitigations |
| RUGGEDCOM RCM1224:<br>All versions >= V6.2 | use TLS v1.3 only |
| SCALANCE LPE9403:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SCALANCE M-800:<br>All versions >= V6.2 | use TLS v1.3 only |
| SCALANCE S602:<br>All versions >= V4.1 | See recommendations from section Workarounds and Mitigations |
| SCALANCE S612:<br>All versions >= V4.1 | See recommendations from section Workarounds and Mitigations |
| SCALANCE S615:<br>All versions >= V6.2 | use TLS v1.3 only |
| SCALANCE S623:<br>All versions >= V4.1 | See recommendations from section Workarounds and Mitigations |
| SCALANCE S627-2M:<br>All versions >= V4.1 | See recommendations from section Workarounds and Mitigations |
| SCALANCE SC-600:<br>All versions >= V2.0 | use TLS v1.3 only |
| SCALANCE W700 IEEE 802.11n:<br>All versions >= V6.5 | See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SCALANCE W1700 IEEE 802.11ac:<br>All versions >= V2.0 | See recommendations from section Workarounds and Mitigations |
| SCALANCE XB-200:<br>All versions < V4.3 | Update to version V4.3<br>https://support.industry.siemens.com/cs/ww/en/view/109799569 |
| SCALANCE XC-200:<br>All versions < V4.3 | Update to version V4.3<br>https://support.industry.siemens.com/cs/ww/en/view/109799569 |
| SCALANCE XF-200BA:<br>All versions < V4.3 | Update to version V4.3<br>https://support.industry.siemens.com/cs/ww/en/view/109799569 |
| SCALANCE XM-400:<br>All versions < V6.4 | Update to version V6.4<br>https://support.industry.siemens.com/cs/ww/en/view/109796319 |
| SCALANCE XP-200:<br>All versions < V4.3 | Update to version V4.3<br>https://support.industry.siemens.com/cs/ww/en/view/109799569 |
| SCALANCE XR-300WG:<br>All versions < V4.3 | Update to version V4.3<br>https://support.industry.siemens.com/cs/ww/en/view/109799569 |
| SCALANCE XR-500 Family:<br>All versions < V6.4 | Update to version V6.4<br>https://support.industry.siemens.com/cs/ww/en/view/109796317 |
| SIMATIC CLOUD Connect 7:<br>All versions >= V1.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC CP 1242-7 GPRS V2:<br>All versions >= V3.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Comfort Panels (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI KTP Mobile Panels:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC Logon:<br>All versions >= V1.6.0.2 | Restrict access to Remote Access service, if used, to mitigate this issue. This service is disabled by default. |

| | |
|---|---|
| SIMATIC MV500:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1243-1 (incl. SIPLUS variants):<br>All versions >= V3.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1243-7 LTE EU:<br>All versions >= V3.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1243-7 LTE US:<br>All versions >= V3.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1243-8 IRC:<br>All versions >= V3.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1542SP-1 IRC (incl. SIPLUS variants):<br>All versions >= 2.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1543-1 (incl. SIPLUS variants):<br>All versions >= V2.2 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1543SP-1 (incl. SIPLUS variants):<br>All versions >= V2.1 | See recommendations from section Workarounds and Mitigations |
| SIMATIC NET CP 1545-1:<br>All versions >= V1.0 | See recommendations from section Workarounds and Mitigations |
| SIMATIC PCS 7 TeleControl:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC PCS neo:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC PDM:<br>All versions >= V9.1.0.7 | Restrict access to the command interface, if used, to mitigate this issue. This interface is disabled by default. |
| SIMATIC Process Historian OPC UA Server:<br>All versions >= 2019 | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF166C:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF185C:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF186C:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF186CI:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF188C:<br>All versions | See recommendations from section Workarounds and Mitigations |

| | |
|---|---|
| SIMATIC RF188CI:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC RF360R:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1200 CPU family (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (MLFB: 6ES7518-4AX00-1AC0, 6AG1518-4AX00-4AC0, incl. SIPLUS variant):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC Runtime Advanced:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC TeleControl:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINAMICS Connect 300:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINEC NMS:<br>V1.0 SP1, V1.0 SP1 Update1 | Update to version V1.0 SP2<br>https://support.industry.siemens.com/cs/ww/en/view/109797645 |
| SINEC PNI:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SINEMA Server V14:<br>V14.0.2, V14.0.2.1, V14.0.2.2 | See recommendations from section Workarounds and Mitigations |
| SINUMERIK OPC UA Server:<br>All versions | See recommendations from section Workarounds and Mitigations |
| TIA Administrator:<br>All versions | See recommendations from section Workarounds and Mitigations |
| TIM 1531 IRC (incl. SIPLUS NET variants):<br>All versions >= V2.0 < V2.2 | Update to version V2.2<br>https://support.industry.siemens.com/cs/ww/en/view/109798331 |

## WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific mitigations or workarounds. Please follow General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

## 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

Products of the SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SCALANCE W700 products are wireless communication devices based on IEEE 802.11 standards. 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 W1700 products are wireless communication devices based on IEEE 802.11 standards. 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 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 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.

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).

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

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 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.

SINEC Product Notification (Primary Network Initialization) is the successor for the Primary Setup tool. In addition to the PROFINET devices, RUGGEDCOM devices can now also be detected and initialized. In addition, network-specific parameters can be set that are necessary for the commissioning of SCALANCE and RUGGEDCOM devices

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.

The Industrial IoT Device SCALANCE LPE (Local Processing Engine) enables data from the manufacturing environment to be acquired, collected, processed and forwarded. At the same time, applications running directly on the device can take over important functions in the plant, for example network services such as DHCP or NTP.

The SCALANCE M-800 / S615 and 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.

The 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.

The SCALANCE SC-600 devices (SC622-2C, 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.

The SCALANCE W1750D controller-based Direct Access Points support radio transmission according to the latest IWLAN standard IEEE 802.11ac Wave 2.

The SIMATIC NET CP 1242-7 and CP 1243-7 LTE communication processors connect the S7-1200 controller to Wide Area Networks (WAN). It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1243-1 communication processor connects the S7-1200 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 SIMATIC NET CP 1243-8 IRC communication processor connects S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC NET CP 1543-1 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 such as FTPs. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

The SIMATIC NET CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors 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 SIMATIC NET 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.

The 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.

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

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.

The software 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.

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

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

## 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.