SSA-179516 OpenSSL Vulnerability in Industrial Products

Publication Date: 2018-08-07
Last Update: 2022-09-13
Current Version: V1.7
CVSS v3.1 Base Score: 5.9

SUMMARY

Several Siemens industrial products are affected by a vulnerability in OpenSSL, that could result in data being sent out unencrypted by the SSL/TLS record layer.

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
MindConnect IoT2040: All versions < V03.01	Update to V03.01 or later version Use the Mindsphere web frontend to update See further recommendations from section Workarounds and Mitigations
MindConnect Nano (IPC227D): All versions < V03.01	Update to V03.01 or later version Use the Mindsphere web frontend to update See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions >= V2.0 < V2.1.6	Update to V2.1.6 or later version https://support.industry.siemens.com/cs/us/en/view/109759122 See further recommendations from section Workarounds and Mitigations
SIMATIC HMI WinCC Flexible: All versions < V15.1	Update to V15.1 or later version https://support.industry.siemens.com/cs/us/en/view/109758794 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagBase: All versions < V2.1.1.0	Update to V2.1.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109792891 See further recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagMonitor: All versions < V5.0.3	Update to V5.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109740915 See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.2.3	Update to V4.2.3 or later version https://support.industry.siemens.com/cs/us/en/view/109741461 Disable web server within the device configuration if it is not used or limit access to the web server on a particular Ethernet/PROFINET port/interface if possible (setting is under General / Web server access). See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.5.2	Update to V2.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109478459 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions >= V2.0 and < V2.6	Update to V2.6 or later version https://support.industry.siemens.com/cs/us/en/view/109478528 See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP2 Update 2	Update to V13 SP2 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109759753 See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V14: All versions < V14 SP1 Update 6	Update to V14 SP1 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109747387 See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V15: All versions < V15 Update 2	Update to V15 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109755826 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V13: All versions < V13 SP2 Update 2	Update to V13 SP2 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109759753 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V14: All versions < V14 SP1 Upd 6	Update to V14 SP1 Upd 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109747387 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V15: All versions < V15 Update 2	Update to V15 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109755826 See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC OA V3.14: All versions < V3.14 P021	Update to V3.14 P021 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.15: All versions < V3.15 P014	Update to V3.15 P014 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.16: All versions < V3.16 P002	Update to V3.16 P002 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SINUMERIK Integrate Access MyMachine service engineer client as part of Sinumerik Integrate Product suite: All versions < V4.1.8	Update to V4.1.8, installing latest Sinumerik Integrate Product suite. The update can be obtained from your local service organization. If assistance in identifying your local service organization is required, please contact a local Siemens hotline center: https://w3.siemens.com/aspa_app See further recommendations from section Workarounds and Mitigations
SINUMERIK Integrate Operate Client as part of Sinumerik Integrate Product suite: All versions <= 2.0.11 / 3.0.11	Update to V2.0.12 / 3.0.12, installing latest Sinumerik Integrate Product suite. The update can be obtained from your local service organization. If assistance in identifying your local service organization is required, please contact a local Siemens hotline center: https://w3.siemens.com/aspa_app 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:

- Limit network access using appropriate mechanisms (e.g., firewalls)

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

MindConnect Nano is a Device for data acquisition via different protocols and permits the transfer of this data to MindSphere.

SIMATIC IPC DiagBase diagnostics software allows to recognize early on any potential faults on SIMATIC IPCs and helps to avoid or reduce system downtimes.

SIMATIC IPC DiagMonitor monitors, reports, visualizes and logs the system states of the SIMATIC IPCs. It communicates with other systems and reacts when events occur.

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.

SIMATIC S7-1500 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC STEP 7 (TIA Portal) is an engineering software to configure and program SIMATIC controllers.

SIMATIC WinCC (TIA Portal) is an engineering software to configure and program SIMATIC Panels, SIMATIC Industrial PCs, and Standard PCs running WinCC Runtime Advanced or SCADA System WinCC Runtime Professional visualization software.

SIMATIC WinCC flexible panels and runtime systems are used for process visualization and control operations.

SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SINUMERIK Integrate product suite facilitates simple networking of machine tools in the IT of the production landscape.

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-2017-3737

In OpenSSL 1.0.2 an “error state” mechanism was introduced. This “error state” mechanism does not work correctly if SSL_read() or SSL_write() is called directly by an application. This could result in data being sent out unencrypted by the SSL/TLS record layer.

Successful exploitation requires an attacker to cause a fatal error in the victim’s SSL/TLS handshake algorithm, and that the targeted application calls SSL_read() or SSL_write() after having already received a fatal error. No user interaction or privileges are required to exploit this security vulnerability. The vulnerability could allow to compromise confidentiality of data by transmitting it unencrypted over the network.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-388: 7PK - Errors

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2018-08-07):	Publication Date
V1.1 (2018-09-11):	Added WinCC OA patches, removed OC1 variant indicator as F is also affected
V1.2 (2018-10-09):	Added update for SIMATIC S7-1200 CPU, SIMATIC STEP 7 (TIA Portal) V13, SIMATIC WinCC (TIA Portal) V13
V1.3 (2018-11-13):	Added update for SIMATIC HMI WinCC Flexible, SIMATIC IPC DiagMonitor
V1.4 (2019-02-12):	Added update for SIMATIC S7-1500 Software Controller, SIMATIC ET 200SP Open Controller CPU 1515SP PC
V1.5 (2019-04-09):	Added update for SIMATIC IPC DiagBase and SIMATIC WinCC (TIA Portal) V14
V1.6 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products
V1.7 (2022-09-13):	Added fix for SIMATIC STEP 7 (TIA Portal) V14; updated fix information for SIMATIC IPC DiagBase and DiagMonitor

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.