SSA-179516: OpenSSL Vulnerability in Industrial Products

Publication Date: 2018-08-07
Last Update: 2019-04-09
Current Version: V1.5
CVSS v3.0 Base Score: 5.9

SUMMARY

A vulnerability in OpenSSL affects several Siemens industrial products. Siemens has released updates for some affected products and is working on updates for others.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
MindConnect IoT2040: All versions < V03.01	Install V03.01 or newer via Mindsphere web frontend
MindConnect Nano (IPC227D): All versions < V03.01	Install V03.01 or newer via Mindsphere web frontend
SIMATIC ET 200SP Open Controller CPU 1515SP PC: All versions >= V2.0 < V2.1.6	Update to V2.1.6 https://support.industry.siemens.com/cs/us/en/view/109759122
SIMATIC HMI WinCC Flexible: All Versions < V15.1	Update to V15.1 https://support.industry.siemens.com/cs/us/en/view/109758794
SIMATIC IPC DiagBase: All versions < V2.1.1.0	Update to V2.1.1.0 https://support.industry.siemens.com/cs/ww/en/view/29316343
SIMATIC IPC DiagMonitor: All Versions < V5.0.3	Update to V5.0.3 Contact customer support to obtain the update
SIMATIC S7-1200: All versions < V4.2.3	Update to V4.2.3 https://support.industry.siemens.com/cs/us/en/view/109741461
SIMATIC S7-1500: All versions < V2.5.2	Update to V2.5.2 https://support.industry.siemens.com/cs/ww/en/view/109478459
SIMATIC S7-1500 Software Controller: All versions >= V2.0 and < V2.6	Update to V2.6 https://support.industry.siemens.com/cs/us/en/view/109478528
SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP2 Update 2	Update to V13 SP2 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109759753
SIMATIC STEP 7 (TIA Portal) V14: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC STEP 7 (TIA Portal) V15: All versions < V15 Update 2	Update to V15 Update 2 or newer https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC WinCC (TIA Portal) V13: All versions < V13 SP2 Update 2	Update to V13 SP2 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109759753
SIMATIC WinCC (TIA Portal) V14: All versions < V14 SP1 Upd 6	Update to V14 SP1 Upd 6 https://support.industry.siemens.com/cs/ww/en/view/109747387
SIMATIC WinCC (TIA Portal) V15: All versions < V15 Update 2	Update to V15 Update 2 or newer https://support.industry.siemens.com/cs/ww/en/view/109755826
SIMATIC WinCC OA V3.14: All versions < V3.14-P021	Update to V3.14-P021 https://portal.etm.at/index.php?option=com_content&view=category&id=67&layout=blog&Itemid=80
SIMATIC WinCC OA V3.15: All versions < V3.15-P014	Update to V3.15-P014 https://portal.etm.at/index.php?option=com_content&view=category&id=68&layout=blog&Itemid=80
SIMATIC WinCC OA V3.16: All versions < V3.16-P002	Update to V3.16-P002 https://portal.etm.at/index.php?option=com_content&view=category&id=69&layout=blog&Itemid=80
SINUMERIK Integrate Access MyMachine service engineer client as part of Sinumerik Integrate Product suite: All versions <= V4.1.7	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
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

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- S7-1200: 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).
- For all other affected products, limit network access using apropriate mechanisms (e.g. firewalls).

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), 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 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.

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

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.

The client-server HMI (human machine interface) system 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.

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

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

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

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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

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.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

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

TERMS OF USE