SSA-701708: Local Privilege Escalation in Industrial Products

Publication Date: 2016-11-07
Last Update: 2018-06-12
Current Version: V1.8
CVSS v3.0 Base Score: 6.4

SUMMARY

In non-default configurations several industrial products are affected by a vulnerability that could allow local Microsoft Windows operating system users to escalate their privileges.

Siemens provides updates for several products and a temporary fix for the remaining affected products. Siemens is working on new versions for the remaining affected products and will update this advisory when new information becomes available.

AFFECTED PRODUCTS AND SOLUTION

If the affected products are installed under their default path (“C:\Program Files*" or the localized equivalent) and the default file system access permissions for drive C:\ were not modified, the security vulnerability is not exploitable.

However, if the affected products are not installed under their default path (“C:\Program Files*" or the localized equivalent), the security vulnerability is potentially exploitable.

Affected Product and Versions	Remediation
Primary Setup Tool (PST): All versions < V4.2 HF1	Update to V4.2 HF1 https://support.industry.siemens.com/cs/ww/en/view/19440762
SIMATIC IT Production Suite: All versions < V7.0 SP1 HFX 2	Update to V7.0 SP1 HFX 2 https://mes-simaticit.siemens.com/tss/html/hfc.html
SIMATIC NET PC-Software: All versions < V14	Upgrade to V14 https://support.industry.siemens.com/cs/ww/en/view/109741996
SIMATIC PCS 7 V7.1 and earlier versions: All versions	Apply temporary fix https://support.industry.siemens.com/cs/ww/en/view/109740929
SIMATIC PCS 7 V8.0: All versions	Apply temporary fix https://support.industry.siemens.com/cs/ww/en/view/109740929
SIMATIC PCS 7 V8.1: All versions	Apply temporary fix and apply SIMATIC WinCC V7.3 Upd 11 https://support.industry.siemens.com/cs/ww/en/view/109740929, https://support.industry.siemens.com/cs/ww/en/view/109742642
SIMATIC PCS 7 V8.2: All versions < V8.2 SP1	Update to V8.2 SP1 To obtain SIMATIC PCS 7 V8.2 SP1 contact your local support.

SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP2	Update to V13 SP2 https://support.industry.siemens.com/cs/ww/en/view/109745155
SIMATIC STEP 7 V5.X: All versions < V5.5 SP4 HF11	Update to V5.5 SP4 HF11 https://support.industry.siemens.com/cs/de/en/view/109737984
SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced: All versions < V14	Upgrade to V14 https://support.industry.siemens.com/cs/ww/en/view/109739719
SIMATIC WinCC (TIA Portal) Professional V13: All versions < V13 SP2	Update to V13 SP2 https://support.industry.siemens.com/cs/ww/en/view/109745155
SIMATIC WinCC (TIA Portal) Professional V14: All versions < V14 SP1	Update to V14 SP1 https://support.industry.siemens.com/cs/ww/en/view/109746074
SIMATIC WinCC Runtime Professional V13: All versions < V13 SP2	Update to V13 SP2 https://support.industry.siemens.com/cs/ww/en/view/109746075
SIMATIC WinCC Runtime Professional V14: All versions < V14 SP1	Update to V14 SP1 https://support.industry.siemens.com/cs/ww/en/view/109746276
SIMATIC WinCC V7.0 SP2 and earlier versions: All versions < V7.0 SP2 Upd 12	Update to V7.0 SP2 Upd 12 https://support.industry.siemens.com/cs/ww/en/view/109741519
SIMATIC WinCC V7.0 SP3: All versions < V7.0 SP3 Upd 8	Update to V7.0 SP3 Upd 8 https://support.industry.siemens.com/cs/ww/en/view/109741127
SIMATIC WinCC V7.2: All versions < V7.2 Upd 14	Update to V7.2 Upd 14 https://support.industry.siemens.com/cs/ww/en/view/109745028
SIMATIC WinCC V7.3: All versions < V7.3 Upd 11	Update to V7.3 Upd 11 https://support.industry.siemens.com/cs/ww/en/view/109742642
SIMATIC WinCC V7.4: All versions < V7.4 SP1	Update to V7.4 SP1 https://support.industry.siemens.com/cs/ww/en/view/109746038
SIMIT V9.0: All versions < V9.0 SP1	Update to V9.0 SP1 https://support.industry.siemens.com/cs/ww/en/view/109743963
SINEMA Remote Connect Client: All versions < V1.0 SP3	Update to V1.0 SP3 https://support.industry.siemens.com/cs/ww/en/view/109754280
SINEMA Server: All versions < V13 SP2	Update to V13 SP2 https://support.industry.siemens.com/cs/ww/en/view/109741833
SOFTNET Security Client V5.0: All versions	Apply temporary fix https://support.industry.siemens.com/cs/ww/en/view/109740929

Security Configuration Tool (SCT): All versions < V4.3 HF1	Update to V4.3 HF1 https://support.industry.siemens.com/cs/ww/en/view/109744041
TeleControl Server Basic: All versions < V3.0 SP2	Update to V3.0 SP2 https://support.industry.siemens.com/cs/ww/en/view/109483119
WinAC RTX 2010 SP2: All versions	Apply temporary fix https://support.industry.siemens.com/cs/ww/en/view/109740929
WinAC RTX F 2010 SP2: All versions	Apply temporary fix https://support.industry.siemens.com/cs/ww/en/view/109740929

WORKAROUNDS AND MITIGATIONS

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

- Install the affected products under their default path ("C:\Program Files*" or the localized equivalent) and verify that file system access permissions for drive C:\\ were not modified.
- Additionally, attackers must have local operating system access to the affected products. Siemens recommends applying Defense-in-Depth (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security) and restricting file system access rights.

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 WinCC is a supervisory control and data acquisition (SCADA) system.

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

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS7 and other components.

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

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 NET PC-Software is required for communication between controllers (PLCs) and PC based solutions (HMIs).

SINEMA Remote Connect ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

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

SIMATIC WinAC RTX is a SIMATIC software controller for PC-based automation solutions.

SIMATIC IT Production Suite is a plant-centric IT solution building the link between Business Systems (e.g. ERP) and Control Systems.

TeleControl Server Basic allows remote monitoring and control of plants.

The SOFTNET Security Client allows programming devices such as PCs and notebook computers to access network nodes or automation systems protected by SCALANCE S.

The simulation software SIMIT allows the simulation of plant setups in order to anticipate faults in the early planning phase.

The Security Configuration Tool (SCT) is an engineering software for security devices such as SCALANCE-S or CP 443-1 Advanced.

The Primary Setup Tool (PST) allows initial network configuration of SIMATIC NET Industrial Ethernet products.

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-2016-7165

Unquoted service paths could allow local Microsoft Windows operating system users to escalate their privileges if the affected products are not installed under their default path ("C:\Program Files*" or the localized equivalent).

CVSS v3.0 Base Score	6.4
CVSS Vector	CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- WATERSURE and KIANDRA IT for coordinated disclosure

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 (2016-11-07):	Publication Date
V1.1 (2016-11-18):	Added update information for WinCC V7.3
V1.2 (2016-12-21):	Added update information for SIMIT V9.0 SP1 and Security Configuration Tool (SCT V4.3 HF1)
V1.3 (2017-02-13):	Added update information for SIMATIC IT Production Suite V7.0 SP1 HFX 2
V1.4 (2017-03-01):	Added update information for SIMATIC WinCC V7.2 and STEP 7 V5.X
V1.5 (2017-05-08):	Added update information for SIMATIC WinCC V7.4, SIMATIC WinCC Runtime Professional, SIMATIC WinCC (TIA Portal) Professional, and SIMATIC STEP 7 (TIA Portal) V13
V1.6 (2017-06-20):	Added update information for Primary Setup Tool (PST)
V1.7 (2018-01-18):	New advisory format, added update information for SINEMA RC Client; Adjusted fix information for PCS 7 V8.1
V1.8 (2018-06-12):	Added update information for PCS 7 V8.2

TERMS OF USE