SSA-701708: Local Privilege Escalation in Industrial Products

Publication Date 2016-11-07
Last Update 2016-11-07
Current Version V1.0
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 under certain conditions.

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

- SIMATIC WinCC:
  - V7.0 SP2 and earlier versions < V7.0 SP2 Upd 12
  - V7.0 SP3: All versions < V7.0 SP3 Upd 8
  - V7.2: All versions
  - V7.3: All versions
  - V7.4: All versions
- SIMATIC STEP 7 V5.X: All versions
- SIMATIC PCS 7
  - V7.1 and earlier versions
  - V8.0: All versions
  - V8.1: All versions
  - V8.2: All versions
- SIMATIC WinCC Runtime Professional: All versions
- SIMATIC WinCC (TIA Portal) Professional: All versions
- SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced: All versions < V14
- SIMATIC STEP 7 (TIA Portal): All versions < V14
- SIMATIC NET PC-Software: All versions < V14
- SINEMA Remote Connect Client: All versions
- SINEMA Server: All versions < V13 SP2
- SIMATIC WinAC RTX 2010 SP2: All versions
- SIMATIC WinAC RTX F 2010 SP2: All versions
- SIMATIC IT Production Suite: All versions
- TeleControl Server Basic: All versions < V3.0 SP2
- SOFTNET Security Client V5.0: All versions
- SIMIT V9.0
- Security Configuration Tool (SCT): All versions
- Primary Setup Tool (PST): All versions

DESCRIPTION

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

SIMATIC STEP 7 V5.X and STEP 7 (TIA Portal) are engineering software for SIMATIC PLC products.

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC.

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

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

SIMATIC WinAC RTX is the 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.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (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 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

Mitigating Factors

The attacker must have local operating system access to the affected products and the affected product must be installed in non-default locations. Siemens recommends applying Defense-in-Depth [9] and restricting file system access rights.

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.

Siemens has released updates for the following products and encourages customers to apply the updates as soon as possible:

- SIMATIC WinCC:
  - V7.0 SP2: and earlier versions: Update to V7.0 SP2 Upd 12 [2]
  - V7.0 SP3: Update to V7.0 SP3 Upd 8 [3]
- SIMATIC WinCC (TIA Portal) Basic, Comfort, Advanced: Upgrade to V14 [4]
- SIMATIC STEP 7 (TIA Portal): Upgrade to V14 [5]
- SIMATIC NET PC-Software: Upgrade to V14 [6]
- TeleControl Server Basic: Update to V3.0 SP2 [7]
- SINEMA Server: Update to V13 SP2 [8]

For the following products in non-default configurations, Siemens provides a temporary fix [1] that resolves the security vulnerability:

- SIMATIC WinCC V7.2
- SIMATIC STEP 7 V5.X
- SIMATIC PCS 7 V7.1 and V8.0
- SIMATIC STEP 7 (TIA Portal) V13
- SIMATIC NET PC-Software V13
- SINEMA Remote Connect Client
- SIMATIC WinAC RTX 2010 SP2
- SIMATIC WinAC RTX F 2010 SP2
- SIMATIC IT Production Suite
- SOFTNET Security Client V5.0
- SIMIT V9.0
- Security Configuration Tool (SCT)
- Primary Setup Tool (PST)

For the following products in non-default configurations, Siemens recommends customers apply the temporary fix [1], follow our operational guidelines [9], and restrict file system access rights:

- SIMATIC WinCC V7.3 and V7.4
- SIMATIC PCS 7 V8.1 and V8.2
- SIMATIC WinCC Runtime Professional
- SIMATIC WinCC (TIA Portal) Professional

Siemens is working on new versions to incorporate the temporary fix for the remaining affected products and will update the advisory when new information becomes available.

As a general security measure Siemens strongly recommends to protect network access to the non-perimeter Industrial Products with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [9] in order to run the products in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks WATERSURE and KIANDRA IT for coordinated disclosure.

ADDITIONAL RESOURCES

[1] The temporary fix can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109740929

[2] SIMATIC WinCC V7.0 SP2 Upd 12 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109741519

[3] SIMATIC WinCC V7.0 SP3 Upd 8 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109741127

[4] SIMATIC WinCC (TIA Portal) V14 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109739719

[5] SIMATIC STEP 7 (TIA Portal) V14 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109740340

[6] SIMATIC NET PC Software V14 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109741996

[7] TeleControl Server Basic V3.0 SP2 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109483119

[8] SINEMA Server V13 SP2 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109741833

[9] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[10] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[11] For further inquiries on 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

DISCLAIMER

See: https://www.siemens.com/terms_of_use