SSA-312271: Unquoted Search Path Vulnerabilities in Windows-based Industrial Software Applications

Publication Date: 2020-06-09
Last Update: 2020-09-08
Current Version: V1.3
CVSS v3.1 Base Score: 6.7

SUMMARY

The latest update for affected products fix local privilege escalation vulnerabilities that could allow authorized local users with administrative privileges to execute custom code with SYSTEM level privileges.

Siemens has released updates for some of the affected products, and is working on further updates. For the remaining affected products, Siemens recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Automation Tool: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET PC software: All versions V16 < V16 Upd3	Update to V16 Upd3 https://support.industry.siemens.com/cs/ww/en/view/109780209/
SIMATIC PCS neo: All versions < V3.0 SP1	Update to V3.0 SP1 To obtain SIMATIC PCS neo V3.0 SP1 contact your local support.
SIMATIC ProSave: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7: All versions < V5.6 SP2 HF3	Update to V5.6 SP2 HF3 https://support.industry.siemens.com/cs/ww/en/view/109779992/
SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP2 Update 4	Update to V13 SP2 Update 4 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	Update to V15.1 Update 5 https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC STEP 7 (TIA Portal) V16: All versions < V16 Update 2	Update to V16 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109775861/

SIMATIC WinCC OA V3.16: All versions < P018	Update to V3.16-P018 or newer https://www.winccoa.com/downloads/category/patches-316.html
SIMATIC WinCC OA V3.17: All versions < P003	Update to V3.17-P003 or newer https://www.winccoa.com/downloads/category/patches-317-1.html
SIMATIC WinCC Runtime Advanced: All versions < V16 Update 2	Update to V16 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109776018
SIMATIC WinCC Runtime Professional V13: All versions < V13 SP2 Update 4	Update to V13 SP2 Update 4 https://support.industry.siemens.com/cs/ww/en/view/109759782
SIMATIC WinCC Runtime Professional V14: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V15: All versions < V15.1 Update 5	Update to V15.1 Update 5 https://support.industry.siemens.com/cs/ww/en/view/109763892
SIMATIC WinCC Runtime Professional V16: All versions < V16 Update 2	Update to V16 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109776017
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Update 14	Update to V7.4 SP1 Update 14 https://support.industry.siemens.com/cs/ww/en/view/109779373
SIMATIC WinCC V7.5: All versions < V7.5 SP1 Update 3	Update to V7.5 SP1 Update 3 https://support.industry.siemens.com/cs/ww/en/view/109773812
SINAMICS STARTER commissioning tool: All versions	See recommendations from section Workarounds and Mitigations
SINAMICS Startdrive: All versions	Update to V16 Update 3 https://support.industry.siemens.com/cs/ww/en/view/109781202
SINEC NMS: All versions	Install the provided patch for the product until a new version is released https://support.industry.siemens.com/cs/ww/en/view/109779600/
SINEMA Server: All versions	Install the provided patch for the product until a new version is released https://support.industry.siemens.com/cs/ww/en/view/109779600/
SINUMERIK ONE virtual: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK Operate: All versions	See 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:

- Make sure that there is no executable at the following locations:
  - *C:\Program.exe*,
  - *C:\Program Files\Common.exe*, or
  - *C:\Program Files\Common Files\Siemens\Automation\Simatic.exe*
- Deactivate the Windows service called *TraceConceptX*. This leads to loss of tracing functionality and should only be considered as a temporary workaround.

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 Automation Tool allows commissioning, adjusting and service in combination with S7-1200 and S7-1500 Controllers without engineering framework.

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

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

SIMATIC PCS neo is a distributed control system (DCS).

SIMATIC ProSave is used for backup restore and firmware update for SIMATIC HMI panels.

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

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.

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

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

STARTER is the drive engineering tool for parameterizing and commissioning.

SINAMICS Startdrive commissioning software is the engineering tool for integration of SINAMICS drives in TIA Portal.

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.

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.

SINUMERIK Operate is a standard Human-Machine-Interface system for SINUMERIK numerical controls.

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-2020-7580

A component within the affected application regularly calls a helper binary with SYSTEM privileges while the call path is not quoted.

CVSS v3.1 Base Score	6.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-428: Unquoted Search Path or Element

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ander Martinez from Titanium Industrial Security for reporting the vulnerabilities
- INCIBE for coordination efforts

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 (2020-06-09):	Publication Date
V1.1 (2020-07-14):	Added solutions for SIMATIC STEP 7 V13, SIMATIC STEP 7 V16, SIMATIC WinCC Runtime Professional V13, SIMATIC WinCC Runtime Professional V16 and SIMATIC WinCC Runtime Advanced
V1.2 (2020-08-11):	Added solution for SIMATIC PCS neo. Errata: SIMATIC PCS 7 removed from affected products
V1.3 (2020-09-08):	Added solution for SINAMICS Startdrive, SIMATIC STEP 7 (TIA Portal) V15, and SIMATIC WinCC Runtime Professional V15

TERMS OF USE