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

Publication Date: 2020-06-09
Last Update: 2022-12-13
Current Version: V2.1
CVSS v3.1 Base Score: 8.8

SUMMARY

Several industrial products as listed below contain a local privilege escalation vulnerability that could allow a local attacker to execute arbitrary code with SYTEM privileges.

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
SIMATIC Automation Tool: All versions < V4 SP2	Update to V4 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/98161300/ See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V14: All versions < V14 SP1 Update 14	Update to V14 SP1 Update 14 or later version https://support.industry.siemens.com/cs/ww/en/view/109807351/ See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V15: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V16: All versions < V16 Upd3	Update to V16 Upd3 or later version https://support.industry.siemens.com/cs/ww/en/view/109780209/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS neo: All versions < V3.0 SP1	Update to V3.0 SP1 or later version To obtain SIMATIC PCS neo V3.0 SP1 contact your local support. See further recommendations from section Workarounds and Mitigations
SIMATIC ProSave: All versions < V17	Update to V17 or later version https://support.industry.siemens.com/cs/ww/en/view/10347815/ Note: Some versions of SIMATIC ProSave are not available as separate download (e.g. V17). In this case, use the version of SIMATIC ProSave as bundled with the corresponding version of SIMATIC WinCC (TIA Portal). See further recommendations from section Workarounds and Mitigations

SIMATIC S7-1500 Software Controller: All versions < V21.8	Update to V21.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V13: All versions < V13 SP2 Update 4	Update to V13 SP2 Update 4 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 10	Update to V14 SP1 Update 10 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 < V15.1 Update 5	Update to V15.1 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/ See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 (TIA Portal) V16: All versions < V16 Update 2	Update to V16 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/ See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V5: All versions < V5.6 SP2 HF3	Update to V5.6 SP2 HF3 or later version https://support.industry.siemens.com/cs/ww/en/view/109779992/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.16: All versions < V3.16 P018	Update to V3.16 P018 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.17: All versions < V3.17 P003	Update to V3.17 P003 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Advanced: All versions < V16 Update 2	Update to V16 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109776018/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V13: All versions < V13 SP2 Update 4	Update to V13 SP2 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109759782/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC Runtime Professional V14: All versions < V14 SP1 Update 10	Update to V14 SP1 Update 10 or later version https://support.industry.siemens.com/cs/ww/en/view/109747394/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V15: All versions < V15.1 Update 5	Update to V15.1 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109763892/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V16: All versions < V16 Update 2	Update to V16 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109776017/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Update 14	Update to V7.4 SP1 Update 14 or later version https://support.industry.siemens.com/cs/ww/en/view/109779373/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.5: All versions < V7.5 SP1 Update 3	Update to V7.5 SP1 Update 3 or later version https://support.industry.siemens.com/cs/ww/en/view/109773812/ See further recommendations from section Workarounds and Mitigations
SINAMICS Startdrive: All Versions < V16 Update 3	Update to V16 Update 3 or later version https://support.industry.siemens.com/cs/ww/en/view/109781202/ See further recommendations from section Workarounds and Mitigations
SINAMICS STARTER: All Versions < V5.4 HF2	Update to V5.4 HF2 or later version https://support.industry.siemens.com/cs/ww/en/view/109782792/ See further recommendations from section Workarounds and Mitigations
SINEC NMS: All versions < V1.0 SP2	Update to version V1.0 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109797645/ See further recommendations from section Workarounds and Mitigations
SINEMA Server: All versions < V14 SP3	Update to V14 SP3 or later version https://support.industry.siemens.com/cs/ww/en/view/109801374/ See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE virtual: All Versions < V6.14	Update to V6.14 or later version The update can be obtained from Siemens representative or via Siemens customer service See further recommendations from section Workarounds and Mitigations

SINUMERIK Operate: All Versions < V6.14	Update to V6.14 or later version The update can be obtained from Siemens representative or via Siemens customer service 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:

- 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.

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

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

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 STEP 7 V5 is the classic engineering software to configure and program SIMATIC S7-300/S7-400/C7/WinAC controllers.

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

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.

STARTER is the drive engineering tool for parameterizing and commissioning.

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 common component used by the affected applications regularly calls a helper binary with SYSTEM privileges while the call path is not quoted.

This could allow a local attacker to execute arbitrary code with SYTEM privileges.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/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:

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

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
V1.4 (2020-12-08): Added solution for SIMATIC S7-1500 Software Controller and SINAMICS STARTER
V1.5 (2021-01-12): Added solution for SIMATIC STEP 7 (TIA Portal) V14 and SIMATIC WinCC Runtime Professional V14
V1.6 (2021-03-09): Added solution for SINUMERIK ONE Virtual and SINUMERIK Operate
V1.7 (2021-06-08): Added solution for SIMATIC Automation Tool and updated solution for SINEC NMS
V1.8 (2021-09-14): Updated solution for SINEMA Server
V1.9 (2021-11-09): Added solution for SIMATIC ProSave
V2.0 (2022-04-12): Added solution for SIMATIC NET PC Software V14 and clarified affected versions
V2.1 (2022-12-13): Corrected description and CVSS score for CVE-2020-7580

TERMS OF USE