

SSA-270778: Denial-of-Service Vulnerability in SIMATIC PCS 7, SIMATIC WinCC and SIMATIC NET PC Software

Publication Date: 2020-02-11
Last Update: 2023-04-11
Current Version: V1.8
CVSS v3.1 Base Score: 7.5

SUMMARY

A Denial-of-Service vulnerability was found in SIMATIC PCS 7, SIMATIC WinCC and SIMATIC NET PC software when encrypted communication is enabled. The vulnerability could allow an attacker with network access to cause a Denial-of-Service condition under certain circumstances (versions prior to SIMATIC WinCC V7.3 or SIMATIC PCS 7 V8.1 are not affected as encrypted communication is not an option).

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

Note: The vulnerability is part of a shared component, used by various Siemens products (SIMATIC Communication Services - SCS). The installation of a fix version of any product also removes the vulnerability for other products on the same system, even if those products were not updated.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenPCS 7 V8.1: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
OpenPCS 7 V8.2: All versions	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 14 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations
OpenPCS 7 V9.0: All versions < V9.0 Upd3	See remediation for SIMATIC PCS 7 V9.0 See further recommendations from section Workarounds and Mitigations
SIMATIC BATCH V8.1: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC BATCH V8.2: All versions < V8.2 Upd12	Update to V8.2 Upd12 or later version https://support.industry.siemens.com/cs/ww/en/view/109757796/ See recommendations from section Workarounds and Mitigations
SIMATIC BATCH V9.0: All versions < V9.0 SP1 Upd5	See remediation for SIMATIC PCS 7 V9.0 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 Update 1	Update to V16 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109778547/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.1: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.2: All versions	Update to V8.2 SP1; then update SIMATIC WinCC to V7.4 SP1 Update 14 or later version on the same system https://support.industry.siemens.com/cs/ww/en/view/109758443/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions < V9.0 SP3	Update to V9.0 SP3 or later version https://support.industry.siemens.com/cs/ww/en/view/109780584/ See further recommendations from section Workarounds and Mitigations
SIMATIC Route Control V8.1: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC Route Control V8.2: All versions	Currently no fix is planned The vulnerability is fixed if SIMATIC WinCC V7.4 SP1 Update 14 or later version is installed on the same system See further recommendations from section Workarounds and Mitigations
SIMATIC Route Control V9.0: All versions < V9.0 Upd4	See remediation for SIMATIC PCS 7 V9.0 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V13: All versions < V13 SP2	Update to V13 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109759782/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V14: All versions < V14 SP1 Update 10	Update to V14 SP1 Update 10 or later version https://support.industry.siemens.com/cs/us/en/view/109747387/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC (TIA Portal) V15.1: All versions < V15.1 Update 5	Update to V15.1 Update 5 or later version https://support.industry.siemens.com/cs/us/en/view/109763890/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V16: All versions < V16 Update 1	Update to V16 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.3: All versions	Currently no fix is planned See 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/us/en/view/109779373/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.5: All versions < V7.5 SP1 Update 1	Update to V7.5 SP1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109773812/ 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:

- Use VPN for protecting network communication between cells

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

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

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

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.

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-2019-19282

Through specially crafted messages, when encrypted communication is enabled, an attacker with network access could use the vulnerability to compromise the availability of the system by causing a Denial-of-Service condition. Successful exploitation requires no system privileges and no user interaction.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-131: Incorrect Calculation of Buffer Size

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Nicholas Miles from Tenable for coordinated disclosure

ADDITIONAL INFORMATION

The vulnerability is part of a shared component, used by various Siemens products (SIMATIC Communication Services - SCS). The installation of a fix version of any product also removes the vulnerability for other products on the same system, even if those products were not updated.

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 (2020-02-11):	Publication Date
V1.1 (2020-03-10):	Added solution for SIMATIC NET PC Software
V1.2 (2020-04-14):	Added solution for SIMATIC WinCC (TIA Portal) V16
V1.3 (2020-05-12):	Added solution for SIMATIC WinCC V7.4
V1.4 (2020-07-14):	Added solution for SIMATIC PCS 7 V9.0
V1.5 (2020-09-08):	Added solution for SIMATIC WinCC (TIA Portal) V15.1
V1.6 (2021-01-12):	Added solution for SIMATIC WinCC (TIA Portal) V14
V1.7 (2022-04-12):	Added solution for SIMATIC PCS 7 V8.2 and related components; added solution for SIMATIC NET PC Software V14 and clarified affected versions; added a note regarding shared components
V1.8 (2023-04-11):	Added fix for SIMATIC BATCH V8.2; updated fix information for OpenPCS 7 V8.2 and SIMATIC Route Control V8.2; added download links for SIMATIC PCS 7 V8.2 SP1 and V9.0 SP3

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.