SSA-348629: Denial-of-Service Vulnerability in SIMATIC PCS 7, SIMATIC WinCC, SIMATIC WinCC Runtime Professional and SIMATIC NET PC Software

Publication Date: 2018-03-27
Last Update: 2022-04-12
Current Version: V1.9
CVSS v3.1 Base Score: 7.5

SUMMARY

A Denial-of-Service vulnerability has been identified in SIMATIC PCS 7, SIMATIC WinCC, SIMATIC WinCC Runtime Professional and SIMATIC NET PC-Software.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenPCS 7 V7.1 and earlier: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
OpenPCS 7 V8.0: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
OpenPCS 7 V8.1: All versions < V8.1 Upd5	Update to OpenPCS 7 V8.1 Upd 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109761055 See further recommendations from section Workarounds and Mitigations
OpenPCS 7 V8.2: All versions	See remediation for PCS 7 V8.2 See further recommendations from section Workarounds and Mitigations
OpenPCS 7 V9.0: All versions < V9.0 Upd1	See remediation for PCS 7 V9.0 See further recommendations from section Workarounds and Mitigations
SIMATIC BATCH V7.1 and earlier: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC BATCH V8.0: All versions < V8.0 SP1 Upd21	Update to SIMATIC BATCH V8.0 SP1 Upd21 or later version https://support.industry.siemens.com/cs/ww/en/view/109756847 See further recommendations from section Workarounds and Mitigations

SIMATIC BATCH V8.1: All versions < V8.1 SP1 Upd16	Update to SIMATIC BATCH V8.1 SP1 Upd16 or later version https://support.industry.siemens.com/cs/ww/en/view/109756846 See further recommendations from section Workarounds and Mitigations
SIMATIC BATCH V8.2: All versions < V8.2 Upd10	Update to SIMATIC BATCH V8.2 Upd10 or later version https://support.industry.siemens.com/cs/ww/en/view/109757796 See further recommendations from section Workarounds and Mitigations
SIMATIC BATCH V9.0: All versions < V9.0 SP1	See remediation for 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 < 15 SP1	Update to V15 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109762690 See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V7.1 and earlier: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.0: All versions	Currently no fix is planned See 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 < V8.2 SP1	Update to V8.2 SP1 or later version To obtain SIMATIC PCS 7 V8.2 SP1 contact your local support. See further recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions < V9.0 SP1	Update to V9.0 SP1 (Includes Open PCS 7 V9.0 Upd1, SIMATIC Batch V9.0 SP1, SIMATIC Route Control V9.0 Upd1 and SIMATIC WinCC V7.4 SP1 Upd4). To obtain SIMATIC PCS 7 V9.0 SP1 contact your local support. See further recommendations from section Workarounds and Mitigations
SIMATIC Route Control V7.1 and earlier: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC Route Control V8.0: All versions	Currently no fix is planned See 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	See remediation for PCS 7 V8.2 See further recommendations from section Workarounds and Mitigations
SIMATIC Route Control V9.0: All versions < V9.0 Upd1	See remediation for PCS 7 V9.0 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V13: All versions < V13 SP2 Upd2	Update to V13 SP2 Upd2 or later version https://support.industry.siemens.com/cs/ww/en/view/109759753 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V14: All versions < V14 SP1 Upd5	Update to V14 SP1 Upd5 or later version https://support.industry.siemens.com/cs/ww/en/view/109747394 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.2 and earlier: All versions < WinCC 7.2 Upd 15	Update to WinCC 7.2 Upd 15 or later version https://support.industry.siemens.com/cs/ww/en/view/109762887 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.3: All versions < WinCC 7.3 Upd 16	Update to WinCC 7.3 Upd 16 or later version https://support.industry.siemens.com/cs/ww/en/view/109756123 See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Upd 4	Update to V7.4 SP1 Upd 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109753031 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:

- Ensure that SIMATIC WinCC, SIMATIC WinCC Runtime Professional and SIMATIC PCS 7 stations communicate via encrypted channels (i.e. activate feature “Encrypted Communication” in SIMATIC WinCC V7.3 or newer and SIMATIC PCS 7 V8.1 or newer). Enabling “Encrypted Communication” completely mitigates the vulnerability.
- 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, OpenPCS7 and other components.

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

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

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-2018-4832

Specially crafted messages sent to the RPC service of the affected products could cause a Denial-of-Service condition on the remote and local communication functionality of the affected products. A reboot of the system is required to recover the remote and local communication functionality.

Please note that an attacker needs to have network access to the Application Server in order to exploit this vulnerability.

At the time of advisory publication no public exploitation of this security vulnerability was known.

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-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Independent researcher cdev1 for coordinated disclosure
- Vladimir Dashchenko from Kaspersky Lab ICS CERT for reporting the vulnerability and 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 (2018-03-27):	Publication Date
V1.1 (2018-04-18):	Updates for SIMATIC BATCH V8.0 and V8.1
V1.2 (2018-06-12):	Updates for PCS 7 8.2
V1.3 (2018-10-09):	Update for OpenPCS 7 V8.1 and SIMATIC WinCC Runtime Professional V13
V1.4 (2018-11-13):	Updated solution for SIMATIC BATCH V8.2, OpenPCS 7 V8.2, SIMATIC Route Control V8.2
V1.5 (2018-12-11):	Updated solution for SIMATIC NET PC-Software
V1.6 (2018-12-13):	Corrected update link for SIMATIC NET PC-Software
V1.7 (2019-01-08):	Updated patch links for WinCC 7.2 and 7.4
V1.8 (2019-03-12):	Corrected fixed version for WinCC 7.4
V1.9 (2022-04-12):	Added solution for SIMATIC NET PC Software V14 and clarified affected versions; Clarified no remediation planned

TERMS OF USE