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: 2018-06-12
Current Version: V1.2
CVSS v3.0 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 that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenPCS 7 V7.1 and earlier: All versions	See recommendations from section Workarounds and Mitigations or upgrade to a newer PCS 7 version
OpenPCS 7 V8.0: All versions	See recommendations from section Workarounds and Mitigations
OpenPCS 7 V8.1: All versions	See recommendations from section Workarounds and Mitigations
OpenPCS 7 V8.2: All versions < V8.2 SP1	See remediation for PCS 7 V8.2
OpenPCS 7 V9.0: All versions < V9.0 Upd1	See remediation for PCS 7 V9.0
SIMATIC BATCH V7.1 and earlier: All versions	See recommendations from section Workarounds and Mitigations or upgrade to a newer PCS 7 version
SIMATIC BATCH V8.0: All versions < SIMATIC BATCH V8.0 SP1 Upd21	Install SIMATIC Batch V8.0 SP1 Upd21. https://support.industry.siemens.com/cs/ww/en/view/109756847
SIMATIC BATCH V8.1: All versions < SIMATIC BATCH V8.1 SP1 Upd16	Install SIMATIC Batch V8.1 SP1 Upd16. https://support.industry.siemens.com/cs/ww/en/view/109756846
SIMATIC BATCH V8.2: All versions < V8.2 SP1	See remediation for PCS 7 V8.2

SIMATIC BATCH V9.0: All versions < V9.0 SP1	See remediation for PCS 7 V9.0
SIMATIC NET PC-Software: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V7.1 and earlier: All versions	See recommendations from section Workarounds and Mitigations or upgrade to a newer PCS 7 version
SIMATIC PCS 7 V8.0: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.2: All versions < V8.2 SP1	Install V8.2 SP1 (Includes SIMATIC WinCC V7.4 SP1 Upd6). To obtain SIMATIC PCS 7 V8.2 SP1 contact your local support.
SIMATIC PCS 7 V9.0: All versions < V9.0 SP1	Install 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.
SIMATIC Route Control V7.1 and earlier: All versions	See recommendations from section Workarounds and Mitigations or upgrade to a newer PCS 7 version
SIMATIC Route Control V8.0: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Route Control V8.1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC Route Control V8.2: All versions < V8.2 SP1	See remediation for PCS 7 V8.2
SIMATIC Route Control V9.0: All versions < V9.0 Upd1	See remediation for PCS 7 V9.0
SIMATIC WinCC Runtime Professional: All versions < V14 SP1 Upd5	Update to V14 SP1 Upd5 https://support.industry.siemens.com/cs/ww/en/view/109747394
SIMATIC WinCC V7.2 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.3: All versions < WinCC 7.3 Upd 16	Update to WinCC 7.3 Upd 16 https://support.industry.siemens.com/cs/ww/en/view/109756123
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Upd4	Update to V7.4 SP1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109753031

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.
- Apply cell protection concept
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth

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 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.

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 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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

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.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

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

TERMS OF USE