SSA-697412: Multiple Vulnerabilities in SIMATIC WinCC, SIMATIC WinCC Runtime, SIMATIC PCS 7, SIMATIC TIA Portal

Publication Date:	2019-05-14
Last Update:	2019-10-08
Current Version:	V1.4
CVSS v3.0 Base Score:	9.1

SUMMARY

The latest update for SIMATIC WinCC fixes multiple vulnerabilities. The most severe could allow an attacker to execute arbitrary commands on an affected system under certain conditions.

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
SIMATIC PCS 7 V8.0 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.1: All versions < V8.1 with WinCC V7.3 Upd 19	Update WinCC to V7.3 Upd 19 https://support.industry.siemens.com/cs/ww/en/view/109768972
SIMATIC PCS 7 V8.2: All versions < V8.2 SP1 with WinCC V7.4 SP1 Upd11	Update WinCC to V7.4 SP1 Upd 11 https://support.industry.siemens.com/cs/ww/en/view/109768093
SIMATIC PCS 7 V9.0: All versions < V9.0 SP2 with WinCC V7.4 SP1 Upd11	Update WinCC to V7.4 SP1 Upd 11 https://support.industry.siemens.com/cs/ww/en/view/109768093
SIMATIC WinCC (TIA Portal) V13: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC (TIA Portal) V14: All versions < V14 SP1 Upd 9	Update to V14 SP1 Upd 9 https://support.industry.siemens.com/cs/ww/en/view/109747387
SIMATIC WinCC (TIA Portal) V15: All versions < V15.1 Upd 3	Update to V15.1 Upd 3 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC WinCC Runtime Professional V13: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V14: All versions < V14.1 Upd 8	Update to V14.1 Upd 8 https://support.industry.siemens.com/cs/ww/en/view/109747394

SIMATIC WinCC Runtime Professional V15: All versions < V15.1 Upd 3	Update to V15.1 Upd 3 https://support.industry.siemens.com/cs/ww/en/view/109763892
SIMATIC WinCC V7.2 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC V7.3: All versions < V7.3 Upd 19	Update to V7.3 Upd 19 https://support.industry.siemens.com/cs/ww/en/view/109768972
SIMATIC WinCC V7.4: All versions < V7.4 SP1 Upd 11	Update to V7.4 SP1 Upd 11 https://support.industry.siemens.com/cs/ww/en/view/109768093
SIMATIC WinCC V7.5: All versions < V7.5 Upd 3	Update to V7.5 Upd 3 https://support.industry.siemens.com/cs/ww/en/view/109767227

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Apply Defense-in-Depth
- Enable “Encrypted communication” in SIMATIC WinCC and SIMATIC PCS 7.
- Only open project files from trusted locations.

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 PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC 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-2019-10916

An attacker with access to the project file could run arbitrary system commands with the privileges of the local database server.

The vulnerability could be exploited by an attacker with access to the project file. The vulnerability does impact the confidentiality, integrity, and availability of the affected system.

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

CVSS v3.0 Base Score	9.1
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2019-10917

An attacker with local access to the project file could cause a Denial-of-Service condition on the affected product while the project file is loaded.

Successful exploitation requires access to the project file. An attacker could use the vulnerability to compromise availability of the affected system.

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

CVSS v3.0 Base Score	3.3
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

Vulnerability CVE-2019-10918

An authenticatd attacker with network access to the DCOM interface could execute arbitrary commands with SYSTEM privileges.

The vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires authentication with a low-privileged user account and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity and availability of the affected system.

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

CVSS v3.0 Base Score	8.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Vladimir Dashchenko and Sergey Temnikov from Kaspersky Lab ICS CERT for coordinated disclosure of vulnerability CVE-2019-10916 and CVE-2019-10917
- CNCERT/CC for coordinated disclosure of vulnerability CVE-2019-10918
- ChengBin Wang from ZheJiang Guoli Security Technology for coordinated disclosure of vulnerability CVE-2019-10918

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 (2019-05-14): Publication Date
V1.1 (2019-07-09): Added update for SIMATIC WinCC V7.4, SIMATIC PCS 7 V8.2 and SIMATIC PCS 7 V9.0
V1.2 (2019-08-13): Added update for SIMATIC WinCC V7.3 and SIMATIC PCS 7 V8.1
V1.3 (2019-09-10): Added update for SIMATIC WinCC Runtime Professional V14 and V15
V1.4 (2019-10-08): Updated remediation for SIMATIC WinCC Runtime Professional V14 and V15 and added update for SIMATIC WinCC (TIA Portal) V14 and SIMATIC WinCC (TIA Portal) V15

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.