SSA-705517: Remote Code Execution Vulnerability in SIMATIC WinCC and SIMATIC PCS 7

Publication Date:	2019-05-14
Last Update:	2019-05-14
Current Version:	V1.0
CVSS v3.0 Base Score:	9.8

SUMMARY

A vulnerability was identified in SIMATIC WinCC and SIMATIC PCS 7, which could allow an unauthenticated attacker with access to the affected devices to execute arbitrary code. The vulnerability can be exploited if the affected systems do not have “Encrypted Communication” enabled.

Siemens provides versions of SIMATIC WinCC and SIMATIC PCS 7, that allow to enable a mode called “Encrypted Communication”, which mitigates the vulnerability.

“Encrypted communication” is enabled by default starting with SIMATIC WinCC V7.5.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7 V8.0 and earlier: All versions	Apply recommendations from Section Workarounds and Mitigations, or upgrade to a newer version and enable “Encrypted Communication”
SIMATIC PCS 7 V8.1 and newer: All versions	Enable “Encrypted Communication”
SIMATIC WinCC V7.2 and earlier: All versions	Apply recommendations from Section Workarounds and Mitigations, or upgrade to a newer version and enable “Encrypted Communication”
SIMATIC WinCC V7.3 and newer: All versions	Enable “Encrypted Communication”. Starting with WinCC V7.5 “Encrypted Communication” is enabled by default

WORKAROUNDS AND MITIGATIONS

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

- Apply Defense-in-Depth concept

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), 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 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-2019-10922

An attacker with network access to affected installations, which are configured without “Encrypted Communication”, can execute arbitrary code.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected installation. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device.

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

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/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

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

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.