SSA-693129: Vulnerability in SIMATIC WinCC and SIMATIC PCS 7

Publication Date	2016-12-09
Last Update	2016-12-09
Current Version	V1.0
CVSS v3.0 Base Score	4.2

SUMMARY

A vulnerability in an ActiveX component of SIMATIC WinCC could allow attackers to crash the affected component or to leak application memory content if a user is tricked into clicking on a malicious link.

AFFECTED PRODUCTS

- SIMATIC WinCC: All versions < SIMATIC WinCC V7.2
- SIMATIC PCS 7: All versions < SIMATIC PCS 7 V8.0 SP1

DESCRIPTION

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system. SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2016-9160)

An attacker could crash an ActiveX component or leak parts of the application memory if a user is tricked into clicking on a malicious link under certain conditions. An attacker must have control over a website that is allowed to execute ActiveX components.

CVSS Base Score	4.2
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:L/E:P/RL:O/RC:C

Mitigating Factors

An attacker must have control over a website that is allowed to execute ActiveX components. Siemens recommends to execute ActiveX components only on trusted sites, and to integrate the software into a “Defense-in-Depth” concept [2].

SOLUTION

Siemens provides SIMATIC WinCC V7.2 [1] and newer, and PCS7 V8.0 SP2 [1] and newer, which fix the vulnerability. Siemens recommends that customers upgrade to the new versions.

As a general security measure Siemens recommends to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Mingzheng Li from Acorn Network Security Lab for coordinated disclosure of the vulnerability.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting the vulnerability and coordination efforts.

ADDITIONAL RESOURCES

[1] SIMATIC WinCC V7.2 and SIMATIC PCS7 V8.0 SP2 can be obtained by contacting your local Siemens representative or customer support:
https://w3.siemens.com/aspa_app/

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2012-12-09): Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use