SSA-523365: Vulnerability in SIMATIC PCS 7

Publication Date 2017-10-18
Last Update 2017-10-18
Current Version V1.0
CVSS v3.0 Base Score 4.9

SUMMARY

The latest software update for SIMATIC PCS 7 fixes a vulnerability, which could allow an attacker to cause a Denial-of-Service (DoS) condition under certain circumstances.

AFFECTED PRODUCTS

- SIMATIC PCS 7:
  - V8.1: All versions < V8.1 SP1 with WinCC V7.3 Upd 13
  - V8.2: All versions

DESCRIPTION

SIMATIC PCS 7 is a distributed control system (DCS).

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system. SIMATIC WinCC Runtime Professional is a human machine interface (HMI).

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-2017-6867)

An authenticated, remote attacker who is member of the “administrators” group could crash services by sending specially crafted messages to the DCOM interface.

CVSS Base Score 4.9
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

Mitigating Factors

The attacker must be member of the group administrators and have network access to an affected system.

SOLUTION

Siemens has released updates for the following product and strongly encourages customers to upgrade to the new versions as soon as possible:

- SIMATIC PCS 7:
  - V8.1: Update to V8.1 SP1 with WinCC V7.3 Upd 13 [1]

Siemens is preparing updates for the remaining affected products and recommends the following mitigations in the meantime:

- Apply cell protection concept [3]

- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [2]

As a general security measure Siemens strongly recommends to protect network access to the SIMATIC PCS 7 stations with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Sergey Temnikov and Vladimir Dashchenko, Critical Infrastructure Defense Team, Kaspersky Lab for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] SIMATIC WinCC V7.3 Upd 13 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746452

[2] SIMATIC PCS 7 and WinCC security concept:
https://support.industry.siemens.com/cs/ww/en/view/60119725

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

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

[5] 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 (2017-10-18): Publication Date

DISCLAIMER