SSA-523365: Vulnerability in SIMATIC PCS 7

Publication Date: 2017-10-18
Last Update: 2018-06-12
Current Version: V1.1
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 AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7 V8.1: All versions < V8.1 SP1 with WinCC V7.3 Upd 13	Update WinCC to V7.3 Upd 13 https://support.industry.siemens.com/cs/ww/en/view/109746452
SIMATIC PCS 7 V8.2: All versions < V8.2 SP1	Update to V8.2 SP1 To obtain SIMATIC PCS 7 V8.2 SP1 contact your local support.

WORKAROUNDS AND MITIGATIONS

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

- 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 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-2017-6867

An authenticated, remote attacker who is member of the "administrators" group couldcrash services by sending specially crafted messages to the DCOM interface.

CVSS v3.0 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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Sergey Temnikov and Vladimir Dashchenko from Critical Infrastructure Defense Team, Kasperky Lab for coordinated disclosure of the vulnerability

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 (2017-10-18):	Publication Date
V1.1 (2018-06-12):	Update of PCS 7 V8.2

TERMS OF USE