SSA-156872: Vulnerability in SIMATIC WinCC and SIMATIC WinCC Runtime Professional

Publication Date 2017-05-08
Last Update 2017-05-08
Current Version V1.0
CVSS v3.0 Base Score 4.9

SUMMARY

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

AFFECTED PRODUCTS

- SIMATIC WinCC:
  - V7.3: All versions < V7.3 Upd 11
  - V7.4: All versions < V7.4 SP1
- SIMATIC WinCC Runtime Professional:
  - V13: All versions < V13 SP2
  - V14: All versions < V14 SP1
- SIMATIC WinCC (TIA Portal) Professional:
  - V13: All versions < V13 SP2
  - V14: All versions < V14 SP1

DESCRIPTION

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

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC (TIA Portal) Professional 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.

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 products and strongly encourages customers to upgrade to the new versions as soon as possible:

- SIMATIC WinCC:
  - V7.3: Update to WinCC V7.3 Update 13 [1]
  - V7.4: Update to WinCC V7.4 SP1 [2]
- SIMATIC WinCC Runtime Professional:
  - V13: Update to V13 SP2 [3]
  - V14: Update to V14 SP1 [4]
- SIMATIC WinCC (TIA Portal) Professional:
  - V13: Update to V13 SP2 [5]
  - V14: Update to V14 SP1 [6]

As a general security measure Siemens strongly recommends to protect network access to the SIMATIC WinCC, SIMATIC WinCC Runtime, and SIMATIC WinCC (TIA Portal) Professional stations with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [7] 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 WinCC V7.4 SP1 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746038

[3] SIMATIC WinCC Runtime Professional V13 SP2 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746268

[4] SIMATIC WinCC Runtime Professional V14 SP1 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746276

[5] SIMATIC WinCC (TIA Portal) Professional V13 SP2 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746075

[6] SIMATIC WinCC (TIA Portal) Professional V14 SP1 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746074

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

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

[9] 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 (2017-05-08): Publication Date

DISCLAIMER

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