SSA-535640: Vulnerability in Industrial Products

Publication Date 2017-08-30
Last Update 2017-11-17
Current Version V1.2
CVSS v3.0 Base Score 8.2

SUMMARY

Various industrial products use the Discovery Service of the OPC UA protocol stack by the OPC foundation [1] and could therefore be affected by the remote resource consumption attacks (CVE-2017-12069).

AFFECTED PRODUCTS

- SIMATIC PCS 7
  - V8.0: All versions
  - V8.1: All versions
- SIMATIC WinCC:
  - V7.2: All versions
- SIMATIC WinCC Runtime Professional:
  - V13: All versions
  - V14: All versions < V14 SP1
- SIMATIC NET PC Software: All versions
- SIMATIC IT Production Suite: All versions between V6.5 (including) and V7.1 (excluding)

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).

SIMATIC NET PC-Software is required for communication between controllers (PLCs) and PC based solutions.

SIMATIC IT Production Suite is a plant-centric IT solution building the link between Business Systems (e.g. ERP) and Control Systems.

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-2017-12069)

By sending specially crafted packets to the OPC Discovery Server at port 4840/tcp, an attacker might cause the system to access various resources chosen by the attacker.

CVSS Base Score 8.2
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have network access to the affected devices. Siemens recommend operating the devices only within trusted networks [5].

SOLUTION

Siemens provides fixes for the following products and recommends customers upgrade to the newest version:

- SIMATIC PCS 7:
  - All affected versions: Follow FAQ [2] to turn off the service after commissioning.
- SIMATIC WinCC:
  - Follow FAQ [2] to turn off the service after commissioning.
- SIMATIC WinCC Runtime Professional:
  - Update to V14 SP1 [3]
  - All other versions: Follow FAQ [2] to turn off the service after commissioning.
- SIMATIC NET PC Software:
  - Follow FAQ [2] to turn off the service after commissioning.
- SIMATIC IT Production Suite:
  - Update to V7.1 [4]

Until patches can be applied, Siemens recommends the following mitigations:

- Turn off the Discovery Service [2] or block it on the local firewall
- Apply cell protection concept [5]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [5]

As a general security measure Siemens strongly recommends to protect network access to the SIMATIC PCS 7 station with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [5] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Sergey Temnikov (Kaspersky Lab ICS CERT)

ADDITIONAL RESOURCES

[1] Original Stack from OPC Foundation: http://opcfoundation.github.io/UA-.NET/
[2] FAQ to turn off LDS after commissioning: https://support.industry.siemens.com/cs/ww/en/view/109749461
[3] SIMATIC WinCC V14 SP1: https://support.industry.siemens.com/cs/ww/en/view/109746276
[4] To obtain SIMATIC IT Production Suite V7.1 contact your local support.

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

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

[7] 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 (2017-08-30): Publication Date
V1.1 (2017-10-02): Clarified “Affected Products”
V1.2 (2017-11-17): Added fix for SIMATIC IT Production Suite

DISCLAIMER