SSA-535640: Vulnerability in Industrial Products

Publication Date: 2017-08-30
Last Update: 2020-08-11
Current Version: V1.4
CVSS v3.1 Base Score: 8.2

SUMMARY

Various industrial products use the Discovery Service of the OPC UA protocol stack by the OPC foundation https://github.com/OPCFoundation/UA-.NETStandard and could therefore be affected by the remote resource consumption attacks (CVE-2017-12069).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC IT Production Suite: All Versions >= V6.5 and < V7.1	Update to V7.1, To optain SIMATIC IT Production Suite V7.1 contact your local support.
SIMATIC NET PC Software: All versions >= V14 and < V15	Update to V15 or later version https://support.industry.siemens.com/cs/ww/en/view/109762690
SIMATIC PCS 7: Versions V8.0, V8.1	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC: All Versions < V7.2	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V13: All Versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional V14: All Versions < V14 SP1	Update to V14 SP1 https://support.industry.siemens.com/cs/ww/en/view/109746276

WORKAROUNDS AND MITIGATIONS

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

- Siemens recommend operating the devices only within trusted networks.
- Turn off the Discovery Service after commissioning or block it on the local firewall: https://support.industry.siemens.com/cs/ww/en/view/109749461
- 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 PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS7 and other components.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

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

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

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

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability 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. To execute the attack, the attacker must have network access to the affected devices.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Sergey Temnikov from Kaspersky Lab ICS CERT for reporting the vulnerabilities

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 (2017-08-30): Publication Date
V1.1 (2017-10-02): Clarified “Affected Products”
V1.2 (2017-11-17): Added fix for SIMATIC IT Production Suite
V1.3 (2019-01-08): Added fix for SIMATIC NET PC Software
V1.4 (2020-08-11): Updated information regarding SIMATIC NET PC Software

TERMS OF USE