SSA-307392: Denial-of-Service in OPC UA in Industrial Products

Publication Date: 2019-04-09
Last Update: 2020-03-10
Current Version: V1.6
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability has been identified in the OPC UA server of several industrial products. The vulnerability could cause a Denial-of-Service condition on the service or the device.

Siemens has released updates for several affected products, and recommends that customers update to the new version. Siemens is preparing further updates and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 443-1 OPC UA: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V2.7	Update to V2.7 https://support.industry.siemens.com/cs/ww/en/view/109759122
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V15.1 Upd 4	Update to V15.1 Upd4 https://support.industry.siemens.com/cs/ww/en/view/109763890
SIMATIC IPC DiagMonitor: All versions < V5.1.3	Update to V5.1.3 https://support.industry.siemens.com/cs/ww/en/view/109763202
SIMATIC NET PC Software: All versions >= V7.1 < V16	Update to V16 https://support.industry.siemens.com/cs/ww/en/view/109775589
SIMATIC RF188C: All versions < V1.1.0	Update to V1.1.0 https://support.industry.siemens.com/cs/ww/en/view/109768507
SIMATIC RF600R: All versions < V3.2.1	Update to V3.2.1 https://support.industry.siemens.com/cs/ww/en/view/109768501

SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions >= V2.5 < V2.6.1	Update to V2.6.1 https://support.industry.siemens.com/cs/ww/en/view/109478459/
SIMATIC S7-1500 Software Controller: All versions between V2.5 (including) and V2.7 (excluding)	Update to V2.7 https://support.industry.siemens.com/cs/ww/en/view/109478528
SIMATIC WinCC OA: All versions < V3.15-P018	Update to V3.15-P018 https://www.winccoa.com/news/detail/new-patch-p018-available-for-315.html
SIMATIC WinCC Runtime Advanced: All versions < V15.1 Upd 4	Update to V15.1 Upd 4 https://support.industry.siemens.com/cs/ww/en/view/109763891
SINEC-NMS: All versions < V1.0 SP1	Update to V1.0 SP1 https://support.industry.siemens.com/cs/ww/en/view/109776939
SINEMA Server: All versions < V14 SP2	Update to V14 SP2 https://support.industry.siemens.com/cs/ww/en/view/109767382
SINUMERIK OPC UA Server: All versions < V2.1	Update to V2.1 or newer https://support.industry.siemens.com/cs/ww/en/view/109746207
TeleControl Server Basic: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Deactivate the OPC UA Service if supported by the product
- 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

The client-server HMI (human machine interface) system SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SINEMA Server is a network monitoring and management software designed by Siemens for use in Industrial Ethernet networks.

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks with up to 12,500 devices.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

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

TeleControl Server Basic allows remote monitoring and control of plants.

SIMATIC IPC DiagMonitor monitors, reports, visualizes and logs the system states of the SIMATIC IPCs. It communicates with other systems and reacts when events occur.

SIMATIC RF600 Readers are used for the contactless identification of every kind of object, e.g. transport containers, pallets, production goods, or it can be generally used for recording goods in bulk.

Communication Processor (CP) modules of families SIMATIC CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2019-6575

Specially crafted network packets sent to affected devices on port 4840/tcp could allow an unauthenticated remote attacker to cause a Denial-of-Service condition of the OPC communication or crash the device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the OPC communication.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-248: Uncaught Exception

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2019-04-09):	Publication Date
V1.1 (2019-05-14):	Clarify productnames for SIMATIC HMI Products, added solution for SIMATIC S7-1500 CPU family, modified affected versions for SIMATIC Net PC Software
V1.2 (2019-06-11):	Added update for SIMATIC Software Controller and SIMATIC ET 200 SP Open Controller CPU 1515SP PC2
V1.3 (2019-07-09):	Added update for SIMATIC RF600R, SIMATIC RF188C and SINEMA Server
V1.4 (2020-01-14):	Added updates for SIMATIC Panels and SIMATIC WinCC Runtime Advanced. SIPLUS devices now explicitly mentioned in the list of affected products
V1.5 (2020-02-11):	Added updates for SIMATIC NET PC Software
V1.6 (2020-03-10):	Added updates for SIMATIC IPC DiagMonitor and SINEC

TERMS OF USE