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

Publication Date: 2019-04-09
Last Update: 2019-05-14
Current Version: V1.1
CVSS v3.0 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 CP443-1 OPC UA: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200 Open Controller CPU 1515SP PC2: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Outdoor Panels 7" & 15": All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Panels 4" - 22": All versions	See recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC IPC DiagMonitor: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software: All versions >= V7.1	See recommendations from section Workarounds and Mitigations
SIMATIC RF188C: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC RF600R: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family: 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 >= V2.5	See recommendations from section Workarounds and Mitigations
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	See recommendations from section Workarounds and Mitigations
SINEC-NMS: All versions	See recommendations from section Workarounds and Mitigations
SINEMA Server: All versions	See recommendations from section Workarounds and Mitigations
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), 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 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.

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-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 v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

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

TERMS OF USE