

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

Publication Date: 2019-04-09  
 Last Update: 2022-08-09  
 Current Version: V1.9  
 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 to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 443-1 OPC UA (6GK7443-1UX00-0XE0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V2.7	Update to V2.7 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109759122">https://support.industry.siemens.com/cs/ww/en/view/109759122</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V15.1 Upd 4	Update to V15.1 Upd4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109763890">https://support.industry.siemens.com/cs/ww/en/view/109763890</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V15.1 Upd 4	Update to V15.1 Upd4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109763890">https://support.industry.siemens.com/cs/ww/en/view/109763890</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V15.1 Upd 4	Update to V15.1 Upd4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109763890">https://support.industry.siemens.com/cs/ww/en/view/109763890</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC IPC DiagMonitor: All versions < V5.1.3	Update to V5.1.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109763202">https://support.industry.siemens.com/cs/ww/en/view/109763202</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC NET PC Software V13: All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>

SIMATIC NET PC Software V14: All versions < V14 SP1 Update 14	Update to V14 SP1 Update 14 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109807351/">https://support.industry.siemens.com/cs/ww/en/view/109807351/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC NET PC Software V15: All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC RF188C (6GT2002-0JE40): All versions < V1.1.0	Update to V1.1.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109768507">https://support.industry.siemens.com/cs/ww/en/view/109768507</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC RF600R family: All versions < V3.2.1	Update to V3.2.1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109768501">https://support.industry.siemens.com/cs/ww/en/view/109768501</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions >= V2.5 < V2.6.1	Update to V2.6.1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109478459/">https://support.industry.siemens.com/cs/ww/en/view/109478459/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-1500 Software Controller: All versions between V2.5 (including) and V2.7 (excluding)	Update to V2.7 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109478528">https://support.industry.siemens.com/cs/ww/en/view/109478528</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC WinCC OA: All versions < V3.15 P018	Update to V3.15 P018 or later version <a href="https://www.winccoa.com/downloads/category/versions-patches.html">https://www.winccoa.com/downloads/category/versions-patches.html</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC WinCC Runtime Advanced: All versions < V15.1 Upd 4	Update to V15.1 Upd 4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109763891">https://support.industry.siemens.com/cs/ww/en/view/109763891</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SINEC NMS: All versions < V1.0 SP1	Update to V1.0 SP1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109776939">https://support.industry.siemens.com/cs/ww/en/view/109776939</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SINEMA Server: All versions < V14 SP2	Update to V14 SP2 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109767382">https://support.industry.siemens.com/cs/ww/en/view/109767382</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

<p>SINUMERIK OPC UA Server: All versions &lt; V2.1</p>	<p>Update to V2.1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109746207">https://support.industry.siemens.com/cs/ww/en/view/109746207</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>
<p>TeleControl Server Basic: All versions &lt; V3.1.1</p>	<p>Update to V3.1.1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109812231/">https://support.industry.siemens.com/cs/ww/en/view/109812231/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a></p>

## **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
- Use VPN for protecting network communication between cells

Product specific remediations or mitigations can be found in the section [Affected Products and Solution](#). Please follow the [General Security Recommendations](#).

## **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 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.

SIMATIC CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

SIMATIC HMI Panels are used for operator control and monitoring of machines and 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 NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

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.

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.

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

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.

TeleControl Server Basic allows remote monitoring and control of plants.

## **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.

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  
V1.7 (2022-02-08):      No remediation planned for SIMATIC CP 443-1 OPC UA  
V1.8 (2022-04-12):      Added solution for SIMATIC NET PC Software V14 and clarified affected versions; no remediation planned for V15  
V1.9 (2022-08-09):      Added fix for TeleControl Server Basic

### **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website ([https://www.siemens.com/terms\\_of\\_use](https://www.siemens.com/terms_of_use), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.