

## SSA-321292: Denial of Service in the OPC Foundation Local Discovery Server (LDS) in Industrial Products

Publication Date: 2022-05-10  
Last Update: 2024-10-08  
Current Version: V1.6  
CVSS v3.1 Base Score: 7.5

### SUMMARY

A vulnerability has been identified in the OPC Foundation Local Discovery Server (LDS) [0] of several industrial products. The vulnerability could cause a denial of service condition on the service or the device.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

[0] <https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2021-40142.pdf>

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenPCS 7 V9.1: All versions affected by <a href="#">CVE-2021-40142</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC NET PC Software:	See below See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC NET PC Software V14: All versions < V14 SP1 Update 14 affected by <a href="#">CVE-2021-40142</a>	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 affected by <a href="#">CVE-2021-40142</a>	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC NET PC Software V16: All versions < V16 Update 6 affected by <a href="#">CVE-2021-40142</a>	Update to V16 Update 6 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109811815/">https://support.industry.siemens.com/cs/ww/en/view/109811815/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

SIMATIC NET PC Software V17: All versions < V17 SP1 affected by <a href="#">CVE-2021-40142</a>	Update to V17 SP1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109808270/">https://support.industry.siemens.com/cs/ww/en/view/109808270/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC Process Historian OPC UA Server: All versions < V2020 SP1 affected by <a href="#">CVE-2021-40142</a>	Update to V2020 SP1 or later version For PCS neo: Update to PCS neo V3.1 SP1 ( <a href="https://support.industry.siemens.com/cs/ww/de/view/109807752/">https://support.industry.siemens.com/cs/ww/de/view/109807752/</a> ) For PCS 7: Update to PCS 7 V9.1 SP1 ( <a href="https://support.industry.siemens.com/cs/ww/en/view/109805073/">https://support.industry.siemens.com/cs/ww/en/view/109805073/</a> ) For WinCC: contact local support See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC WinCC: All versions < V8.0 affected by <a href="#">CVE-2021-40142</a>	Update to V8.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816599/">https://support.industry.siemens.com/cs/ww/en/view/109816599/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC WinCC Runtime Professional: All versions < V18 affected by <a href="#">CVE-2021-40142</a>	Update to V18 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109813587/">https://support.industry.siemens.com/cs/ww/en/view/109813587/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
TeleControl Server Basic V3: All versions < V3.1.1 affected by <a href="#">CVE-2021-40142</a>	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>
Totally Integrated Automation Portal (TIA Portal):	Update to V18 Update 1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109807123/">https://support.industry.siemens.com/cs/ww/en/view/109807123/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
Totally Integrated Automation Portal (TIA Portal) V18:	Update to V18 Update 1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109807123/">https://support.industry.siemens.com/cs/ww/en/view/109807123/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC WinCC Unified PC Runtime V18: All versions < V18 Update 1 affected by <a href="#">CVE-2021-40142</a>	Update to V18 Update 1 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109807123/">https://support.industry.siemens.com/cs/ww/en/view/109807123/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

## **WORKAROUNDS AND MITIGATIONS**

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

- Deactivate the OPC LDS Service if supported by the product use case. The LDS service is not activated in the default configuration
- 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**

OpenPCS 7 is an OPC-compliant connection to business planning and operations control systems. OpenPCS 7 provides a direct connection to MES and MOM systems.

SIMATIC Process Historian is the long term archive system for SIMATIC PCS 7, SIMATIC WinCC and SIMATIC PCS neo. It stores process values, alarms and batch data of production plants in its database and offers historical process data to reporting and visualization applications.

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

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 WinCC Unified PC Runtime is the new visualization runtime platform used for operator control and monitoring of machines and plants.

TeleControl Server Basic allows remote monitoring and control of plants.

## **VULNERABILITY DESCRIPTION**

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### **Vulnerability CVE-2021-40142**

In OPC Foundation Local Discovery Server (LDS) before 1.04.402.463, remote attackers can cause a denial of service condition by sending carefully crafted messages that lead to access of a memory location after the end of a buffer.

CVSS v3.1 Base Score	7.5
CVSS Vector	<a href="#">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</a>
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

## **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 (2022-05-10):	Publication Date
V1.1 (2022-07-12):	Added fix for SIMATIC NET PC Software V16
V1.2 (2022-08-09):	Added fix for TeleControl Server Basic
V1.3 (2022-12-13):	Added fix for SIMATIC WinCC Runtime Professional and SIMATIC WinCC Unified PC Runtime
V1.4 (2023-03-14):	Added OpenPCS 7 to the list of affected products
V1.5 (2023-04-11):	Added fix for SIMATIC WinCC
V1.6 (2024-10-08):	Added OpenPCS 7 affected version and clarified no fix planned for OpenPCS 7 V9.1

## **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.