SSA-691715: Vulnerability in OPC Foundation Local Discovery Server Affecting Siemens Products

Publication Date:	2023-04-11
Last Update:	2024-04-09
Current Version:	V1.4
CVSS v3.1 Base Score:	7.8

SUMMARY

A vulnerability was identified in OPC Foundation Local Discovery Server which also affects Siemens products that could allow an attacker to escalate privileges under certain circumstances.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OpenPCS 7 V9.1: All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V14: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V15: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V16: All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V17: All versions < V17 SP1 affected by all CVEs	Update to V17 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109808270/ See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V18: All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC Process Historian 2020 OPC UA Server: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC Process Historian 2022 OPC UA Server: All versions < V2022 SP1 affected by all CVEs	In the context of SIMATIC PCS neo, update to SIMATIC PCS neo V4.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109825230/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC: All versions < V8.0 affected by all CVEs	Update to V8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109816599/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Runtime Professional: All versions < V18 Update 2 affected by all CVEs	Update to V18 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109807225/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Unified PC Runtime: All versions < V18.0 SP1 Update 1 affected by all CVEs	Update to V18.0 SP1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807123/ See further recommendations from section Workarounds and Mitigations
TeleControl Server Basic V3: All versions < V3.1.2 affected by all CVEs	Update to V3.1.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109955177/ See further 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:

- Update the underlying OPC Foundation Unified Architecture Local Discovery Server (UA-LDS) to [V1.04.405](https://opcfoundation.org/developer-tools/samples-and-tools-unified-architecture/local-discovery-server-lds/) or later if possible

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 PCS 7 TeleControl is a server based software for the integration of outstations for monitoring and controlling highly remote plant units (referred to as RTUs, usually with a small or medium degree of automation) into the PCS 7 control system. This is carried out by means of telecontrol protocols over a WAN (Wide Area Network).

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

SIMATIC WinCC Unified is a completely new visualization system that enables you to successfully master the challenges of digitization in machine and plant engineering.

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-2022-44725

OPC Foundation Local Discovery Server (LDS) in affected products uses a hard-coded file path to a configuration file. This allows a normal user to create a malicious file that is loaded by LDS (running as a high-privilege user).

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Heinzl for coordinated disclosure

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 (2023-04-11):	Publication Date
V1.1 (2023-06-13):	Added fix for SIMATIC NET PC Software V17, clarified no fix planned for SIMATIC Process Historian 2020 OPC UA Server, SIMATIC NET PC Software V14 and V15
V1.2 (2023-08-08):	Added fix for SIMATIC WinCC Runtime Professional
V1.3 (2023-11-14):	Added fix for SIMATIC Process Historian 2022 OPC UA Server
V1.4 (2024-04-09):	Added fix for TeleControl Server Basic V3

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, 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.