SSA-508677: Use of Obsolete Function Vulnerability in SIMATIC WinCC before V8

Publication Date: 2023-06-13
Last Update: 2023-06-13
Current Version: V1.0
CVSS v3.1 Base Score: 3.9

SUMMARY

Before SIMATIC WinCC V8, legacy OPC services (OPC DA (Data Access), OPC HDA (Historical Data Access), and OPC AE (Alarms & Events)) were used per default. These services were designed on top of the Windows ActiveX and DCOM mechanisms and do not implement state-of-the-art security mechanisms for authentication and encryption of contents.

Starting with WinCC V8.0 the legacy OPC services are no longer enabled by default in new installations. Siemens recommends to use OPC UA instead and to disable the legacy OPC services. For deployments where the legacy OPC services are still in use, ensure that only trusted users are part of the SIMATIC HMI group.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC NET PC Software V14: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V15: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V8.2: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.1: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC WinCC: All versions < V8.0	Update to V8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109816599/ See recommendations from section Workarounds and Mitigations
SINAUT Software ST7sc: All versions	Currently no fix is planned 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:

- SINATIC NET PC Software: Ensure that only trusted users are part of the SIMATIC Net group
- Disable the legacy OPC DA/HDA/AE services and switch to OPC UA, if possible
- Ensure that only trusted users are part of the SIMATIC HMI group

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

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS 7 and other components.

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

SINAUT Software ST7sc connects SINAUT ST7 stations to HMI, SCADA and office applications via OPC.

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-2023-28829

Before SIMATIC WinCC V8, legacy OPC services (OPC DA (Data Access), OPC HDA (Historical Data Access), and OPC AE (Alarms & Events)) were used per default. These services were designed on top of the Windows ActiveX and DCOM mechanisms and do not implement state-of-the-art security mechanisms for authentication and encryption of contents.

CVSS v3.1 Base Score	3.9
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-477: Use of Obsolete Function

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 (2023-06-13): Publication Date

TERMS OF USE