SSA-111512: Client-side Authentication in SIMATIC WinCC OA

Publication Date:	2022-06-21
Last Update:	2022-06-21
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

SIMATIC WinCC OA implements client-side only authentication, when neither server-side authentication (SSA) nor Kerberos authentication is enabled. In this configuration, attackers could impersonate other users or exploit the client-server protocol without being authenticated.

Siemens recommends to enable server-side authentication (SSA) or Kerberos authentication for all WinCC OA projects, as documented in the WinCC OA Security Guideline. In SIMATIC WinCC OA server-side authentication is available since V3.15 (and offered as the default configuration since V3.17). Additional information can be found at: https://cert-portal.siemens.com/productcert/news.html?id=21.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC OA V3.16: All versions in default configuration	Enable server-side authentication (SSA) or Kerberos authentication for your WinCC OA project https://www.winccoa.com/downloads/detail/security-guideline-wincc-oa-v316-1.html
SIMATIC WinCC OA V3.17: All versions in non-default configuration	Ensure that server-side authentication (SSA) is enabled for your WinCC OA project (which is the default configuration); alternatively enable Kerberos authentication https://www.winccoa.com/downloads/detail/security-guideline-wincc-oa-v317.html
SIMATIC WinCC OA V3.18: All versions in non-default configuration	Ensure that server-side authentication (SSA) is enabled for your WinCC OA project (which is the default configuration); alternatively enable Kerberos authentication https://www.winccoa.com/downloads/detail/security-guideline-wincc-oa-v318.html

WORKAROUNDS AND MITIGATIONS

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 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.

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-2022-33139

Affected applications use client-side only authentication, when neither server-side authentication (SSA) nor Kerberos authentication is enabled.

In this configuration, attackers could impersonate other users or exploit the client-server protocol without being authenticated.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-603: Use of Client-Side Authentication

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Daniel dos Santos and Jos Wetzels from Forescout Technologies for coordinated disclosure

ADDITIONAL INFORMATION

In SIMATIC WinCC OA server-side authentication is available since V3.15 (and offered as the default configuration since V3.17). Find additional information at: https://cert-portal.siemens.com/productcert/news.html?id=21.

This issue is also addressed, among other findings across the OT industry, in a recent article from Forescout Vedere Labs, dubbed as “OT:ICEFALL”: https://www.forescout.com/research-labs/ot-icefall/

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 (2022-06-21):	Publication Date

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.