SSA-547714: Argument Injection Vulnerability in SIMATIC WinCC OA Ultralight Client

Publication Date: 2022-12-13
Last Update: 2023-01-10
Current Version: V1.1
CVSS v3.1 Base Score: 5.4

SUMMARY

SIMATIC WinCC OA contains an argument injection vulnerability that could allow an authenticated remote attacker to inject arbitrary parameters, when starting the Ultralight Client via the web interface (e.g., open attacker chosen panels with the attacker's credentials or start a Ctrl script).

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC OA V3.15: All versions < V3.15 P038	Update to V3.15 P038 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.16: All versions < V3.16 P035	Update to V3.16 P035 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.17: All versions < V3.17 P024	Update to V3.17 P024 or later version https://www.winccoa.com/downloads/category/versions-patches.html See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC OA V3.18: All versions < V3.18 P014	Update to V3.18 P014 or later version https://www.winccoa.com/downloads/category/versions-patches.html 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:

- Configure user permissions and access management according to the WinCC OA Security Guideline: https://www.winccoa.com/documentation/WinCCOA/3.18/en_US/UserAdmin/security.html

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-2022-44731

The affected component allows to inject custom arguments to the Ultralight Client backend application under certain circumstances.

This could allow an authenticated remote attacker to inject arbitrary parameters when starting the client via the web interface (e.g., open attacker chosen panels with the attacker's credentials or start a Ctrl script).

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

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 (2022-12-13): Publication Date
V1.1 (2023-01-10): Added fix for SIMATIC WinCC OA V3.15

TERMS OF USE