SSA-914026: Local Code Execution Vulnerability in SIMATIC WinCC V7

Publication Date: 2023-06-13
Last Update: 2023-06-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

SIMATIC WinCC V7 is affected by a vulnerability that could allow a local attacker to inject arbitrary code and escalate privileges, if a non-default installation path was chosen during installation.

Siemens has released an update for SIMATIC WinCC and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC: All versions < V7.5.2.13	Update to V7.5.2.13 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/ 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:

- Harden the application server to prevent local access by untrusted personnel
- After installation to a non-default folder, ensure that the access permissions of that folder are equal to the permissions of the `Program Files` folder
- Always use the default installation path when installing SIMATIC WinCC V7

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

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-2023-30897

Affected applications fail to set proper access rights for their installation folder if a non-default installation path was chosen during installation.

This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.

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-732: Incorrect Permission Assignment for Critical Resource

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Mustafa Mert Konduz from Siemens Energy for reporting the vulnerability

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