SSA-313488: Multiple Vulnerabilities in SIMATIC CN 4100 before V2.5

Publication Date: 2023-07-11
Last Update: 2023-07-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

SIMATIC CN 4100 is vulnerable to improper access control and insecure default configurations that could allow an attacker to gain privilege escalation, and bypass network isolation.

Siemens has released an update for SIMATIC CN 4100 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CN 4100: All versions < V2.5	Update to V2.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109814144/

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

The SIMATIC CN 4100 is a communication node that allows connecting third-party systems helping to implement system concepts for process control technology.

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-2023-29130

Affected device consists of improper access controls in the configuration files that leads to privilege escalation. An attacker could gain admin access with this vulnerability leading to complete device control.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2023-29131

Affected device consists of an incorrect default value in the SSH configuration. This could allow an attacker to bypass network isolation.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-276: Incorrect Default Permissions

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Klassen and Martin Floeck from BASF Security Team for reporting the vulnerabilities

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 (2023-07-11): Publication Date

TERMS OF USE