# SSA-777015: Multiple Vulnerabilities in SIMATIC CN 4100 before V2.7

Publication Date: 2024-01-09
Last Update: 2024-01-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

## SUMMARY

SIMATIC CN 4100 is vulnerable to authorization bypass through user-controlled key, use of default credentials and unauthenticated IP address change that could allow an attacker to remotely login as root or cause denial of service condition of the device.

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

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC CN 4100:<br>All versions < V2.7 | Update to V2.7 or later version<br>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-2023-49251

The "intermediate installation" system state of the affected application allows an attacker to add their own login credentials to the device. This allows an attacker to remotely login as root and take control of the device even after the affected device is fully set up.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-639: Authorization Bypass Through User-Controlled Key |

### Vulnerability CVE-2023-49252

The affected application allows IP configuration change without authentication to the device. This could allow an attacker to cause denial of service condition.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-49621

The "intermediate installation" system state of the affected application uses default credential with admin privileges. An attacker could use the credentials to gain complete control of the affected device.

| | |
|---|---|
| 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-1392: Use of Default Credentials |

## 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 (2024-01-09): Publication Date

## TERMS OF USE