SSA-626991: Denial of Service Vulnerability in SIMATIC CN 4100 before V4.0

Publication Date: 2025-07-08
Last Update: 2025-07-08
Current Version: V1.0
CVSS v3.1 Base Score: 6.5
CVSS v4.0 Base Score: 7.1

SUMMARY

A vulnerability in SIMATIC CN 4100 could allow an attacker to cause a denial of service condition.

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: All versions < V4.0 affected by CVE-2025-40593	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814144/

WORKAROUNDS AND MITIGATIONS

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2025-40593

The affected application allows to control the device by storing arbitrary files in the SFTP folder of the device. This could allow an attacker to cause a denial of service condition.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score	7.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Michael Klassen and Martin Floeck from BASF Security Team 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 (2025-07-08):	Publication Date

TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.