

SSA-178380: Denial-of-Service Vulnerability in SINUMERIK Controllers

Publication Date: 2021-10-12
Last Update: 2021-10-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

A Denial-of-Service vulnerability found in SINUMERIK Controllers could allow an unauthenticated attacker with network access to the affected devices to cause system failure with total loss of availability.

Siemens has released an update for the SINUMERIK 828D and recommends to update to the latest version. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK 808D: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK 828D: All versions < V4.95	Update to V4.95 or later version The update can be obtained from your Siemens representative or via Siemens customer service.

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to port 102/tcp to trusted systems e.g. with an external firewall
- Apply general workarounds.

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

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

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-2021-37199

Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

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-122: Heap-based Buffer Overflow

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Industrial Control Security Laboratory of Qi An Xin Group Inc. for reporting the vulnerability and coordination efforts

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 (2021-10-12): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.