

SSA-337210: Privilege Escalation Vulnerability in SINUMERIK MC

Publication Date: 2022-03-08
Last Update: 2022-03-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

The NC plug-in card in SINUMERIK MC contains a privilege escalation vulnerability that could allow local attackers to escalate their privileges to root. This allows full access to the device, including read and modifying G code.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK MC: All versions < V1.15 SP1	Update to V1.15 SP1 or laterj version SINUMERIK software can be obtained from your local Siemens account manager.
SINUMERIK ONE: All versions < V6.15 SP1	Update to V6.15 SP1 or later version SINUMERIK software can be obtained from your local Siemens account manager.

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the [General Security Recommendations](#).

Product specific mitigations can be found in the section [Affected Products and Solution](#).

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 MC is a CNC system for customized machine solutions.

SINUMERIK ONE is a digital-native CNC 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-2022-24408

The sc SUID binary on affected devices provides several commands that are used to execute system commands or modify system files.

A specific set of operations using sc could allow local attackers to escalate their privileges to root.

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-269: Improper Privilege Management

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 (2022-03-08): 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.