



CVE-2021-37199

Published on: 10/12/2021 12:00:00 AM UTC

Last Modified on: 10/19/2021 11:55:00 AM UTC

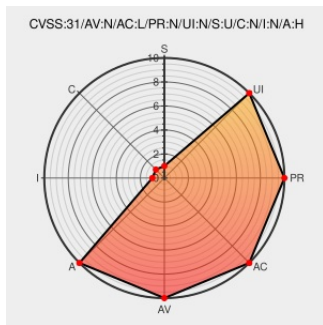
CVE-2021-37199

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Sinumerik 808d](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SINUMERIK 808D (All versions), SINUMERIK 828D (All versions < V4.95). 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.

CVE-2021-37199 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) **Siemens** - **SINUMERIK 808D** version **All versions**

Affected Vendor/Software: [S](#) **Siemens** - **SINUMERIK 828D** version **All versions < V4.95**

CVSS3 Score: **7.5 - HIGH**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|------------------|------------------------|---------------------|---------------------|
| NETWORK | LOW | NONE | NONE |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| UNCHANGED | NONE | NONE | HIGH |

CVSS2 Score: **7.8 - HIGH**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | LOW | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| NONE | NONE | COMPLETE |

CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

cert-portal.siemens.com
application/pdf



MISC cert-portal.siemens.com/productcert/pdf/ssa-178380.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590580 Siemens SINUMERIK Heap-based Buffer Overflow Vulnerability (ICSA-21-287-04)

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|--|-------------------------|---|---------|--------|---------|----------|
| Hardware  | Siemens | Sinumerik 808d | - | All | All | All |
| Operating System | Siemens | Sinumerik 808d Firmware | All | All | All | All |
| Hardware  | Siemens | Sinumerik 828d | - | All | All | All |
| Operating System | Siemens | Sinumerik 828d Firmware | All | All | All | All |

cpe:2.3:h:siemens:sinumerik_808d:-:*:*:*:*:*:

cpe:2.3:o:siemens:sinumerik_808d_firmware:*:*:*:*:*:

cpe:2.3:h:siemens:sinumerik_828d:-:*:*:*:*:*:

cpe:2.3:o:siemens:sinumerik_828d_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|--|--|---------------------|
|  @CVEreport | CVE-2021-37199 : A vulnerability has been identified in SINUMERIK 808D All versions , SINUMERIK 828D All versions... twitter.com/i/web/status/1... | 2021-10-12 09:58:21 |

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)