



# CVE-2013-2829

Published on: 02/13/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:41 PM UTC

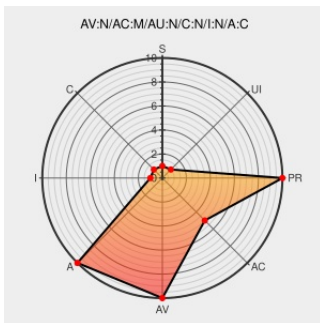
## CVE-2013-2829

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Scada Dnp3 Opc Server](#) from [Matrikonopc](#) contain the following vulnerability:

MatrikonOPC SCADA DNP3 OPC Server 1.2.2.0 and earlier allows remote attackers to cause a denial of service (infinite loop) via a malformed DNP3 packet.

CVE-2013-2829 has been assigned by [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) to track the vulnerability

CVSS2 Score: **7.1 - HIGH**

Access  
Vector

Access  
Complexity

Authentication

**NETWORK**

**MEDIUM**

**NONE**

Confidentiality  
Impact

Integrity  
Impact

Availability  
Impact

**NONE**

**NONE**

**COMPLETE**

## CVE References

Description

Tags

Link

MatrikonOPC Improper Input Validation | ICS-CERT

[US Government Resource](#)  
[ics-cert.us-cert.gov](https://ics-cert.us-cert.gov)  
[text/html](#)

[MISC ics-cert.us-cert.gov/advisories/ICSA-14-010-01](https://ics-cert.us-cert.gov/advisories/ICSA-14-010-01)

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                         | Vendor                      | Product                               | Version                   | Update | Edition | Language |
|--------------------------------------------------------------|-----------------------------|---------------------------------------|---------------------------|--------|---------|----------|
| Application                                                  | <a href="#">Matrikonopc</a> | <a href="#">Scada Dnp3 Opc Server</a> | 1.2.0                     | All    | All     | All      |
| Application                                                  | <a href="#">Matrikonopc</a> | <a href="#">Scada Dnp3 Opc Server</a> | 1.2.0                     | All    | All     | All      |
| Application                                                  | <a href="#">Matrikonopc</a> | <a href="#">Scada Dnp3 Opc Server</a> | All                       | All    | All     | All      |
| cpe:2.3:a:matrikonopc:scada_dnp3_opc_server:1.2.0:*:*:*:*:*: |                             |                                       |                           |        |         |          |
| cpe:2.3:a:matrikonopc:scada_dnp3_opc_server:1.2.0:*:*:*:*:*: |                             |                                       |                           |        |         |          |
| cpe:2.3:a:matrikonopc:scada_dnp3_opc_server:*:*:*:*:*:       |                             |                                       |                           |        |         |          |
| No vendor comments have been submitted for this CVE          |                             |                                       |                           |        |         |          |
| <a href="#">← Previous ID</a>                                |                             |                                       | <a href="#">Next ID →</a> |        |         |          |