



CVE-2022-25231

Published on: Not Yet Published

Last Modified on: 08/26/2022 01:01:00 PM UTC

CVE-2022-25231

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P



Certain versions of [Node-opcua](#) from [Node-opcua Project](#) contain the following vulnerability:

The package node-opcua before 2.74.0 are vulnerable to Denial of Service (DoS) by sending a specifically crafted OPC UA message with a special OPC UA NodeID, when the requested memory allocation exceeds the v8's memory limit.

CVE-2022-25231 has been assigned by [report@snyk.io](#) to track the vulnerability - currently rated as **HIGH** severity.

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

CVE References

Description	Tags	Link
server: use ServiceFault on request error · node-opcua/node-opcua@7b5044b · GitHub	github.com text/html	MISC github.com/node-opcua/node-opcua/commit/7b5044b3f5866fbedc3efabd05e407352c07bd2f
Denial of Service (DoS) in node-opcua CVE-2022-25231 Snyk	security.snyk.io text/html	MISC security.snyk.io/vuln/SNYK-JS-NODEOPCUA-2988724
Use service fault by erossignon · Pull Request #1182 · node-opcua/node-opcua · GitHub	github.com text/html	MISC github.com/node-opcua/node-opcua/pull/1182

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](#).

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Node-opcua Project	Node-opcua	All	All	All	All
cpe:2.3:a:node-opcua_project:node-opcua:*:*:*:*:node.js:*:*:						

Discovery Credit

Vera Mens

Uri Katz

Sharon Brizinov of Team82 (Claroty Research)

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-25231 : The package node-opcua before 2.74.0 are vulnerable to Denial of Service #DoS by sending a speci... twitter.com/i/web/status/1...	2022-08-23 05:16:17
 @threatmeter	CVE-2022-25231 The package node-opcua before 2.74.0 are vulnerable to Denial of Service (DoS) by sending a specific... twitter.com/i/web/status/1...	2022-08-24 07:09:18
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-25231 - The package node-opcua before 2.74.0 are vulnerable to Denial of Serv... twitter.com/i/web/status/1...	2022-08-26 13:12:15
 /r/netcve	CVE-2022-25231	2022-08-23 05:38:51

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)