



CVE-2021-29469

Published on: 04/23/2021 12:00:00 AM UTC

Last Modified on: 08/03/2022 10:23:00 AM UTC

CVE-2021-29469 - advisory for GHSA-35q2-47q7-3pc3

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

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



Certain versions of [Redis](#) from [Redis.js](#) contain the following vulnerability:

Node-redis is a Node.js Redis client. Before version 3.1.1, when a client is in monitoring mode, the regex begin used to detected monitor messages could cause exponential backtracking on some strings. This issue could lead to a denial of service. The issue is patched in version 3.1.1.

CVE-2021-29469 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [NodeRedis](#) - **node-redis** version < 3.1.1

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: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Release V3.1.1 · NodeRedis/node-redis · GitHub	github.com	MISC github.com/NodeRedis/node-

	text/html	redis/releases/tag/v3.1.1
CVE-2021-29469 Node.js Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20210611-0010/
fix #1569 - improve monitor_regex (#1595) · NodeRedis/node-redis@2d11b6d · GitHub	github.com text/html	 MISC github.com/NodeRedis/node-redis/commit/2d11b6dc9b9774464a91fb4b448bad8bf699629e
Potential exponential regex in monitor mode · Advisory · NodeRedis/node-redis · GitHub	github.com text/html	 CONFIRM github.com/NodeRedis/node-redis/security/advisories/GHSA-35q2-47q7-3pc3
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

[179702](#) Debian Security Update for node-redis (CVE-2021-29469)

[982277](#) Nodejs (npm) Security Update for redis (GHSA-35q2-47q7-3pc3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redis.js	Redis	All	All	All	All
cpe:2.3:a:redis.js:redis:*:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← 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](#)