

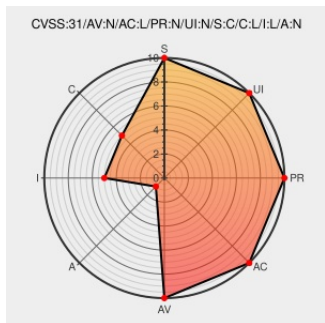


CVE-2021-21304

Published on: 02/08/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 03:44:00 PM UTC

CVE-2021-21304 - advisory for GHSA-rrqm-p222-8ph2

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

Certain versions of [Dynamoose](#) from [Dynamoosejs](#) contain the following vulnerability:

Dynamoose is an open-source modeling tool for Amazon's DynamoDB. In Dynamoose from version 2.0.0 and before version 2.7.0 there was a prototype pollution vulnerability in the internal utility method "lib/utls/object/set.ts". This method is used throughout the codebase for various operations throughout Dynamoose. We have not seen any

evidence of this vulnerability being exploited. There is no evidence this vulnerability impacts versions 1.x.x since the vulnerable method was added as part of the v2 rewrite. This vulnerability also impacts v2.x.x beta/alpha versions. Version 2.7.0 includes a patch for this vulnerability.

CVE-2021-21304 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [dynamoose](#) - dynamoose version $\geq 2.0.0$, $< 2.7.0$

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-rrqm-p222-8ph2 · dynamoose/dynamoose@324c62b · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/dynamoose/dynamoose/commit/324c62b4709204955931a187362f899
Prototype Pollution · Advisory · dynamoose/dynamoose · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/dynamoose/dynamoose/security/advisories/GHSA-rrqm-p222-8ph2
dynamoose	Product Third Party Advisory www.npmjs.com text/html	 MISC www.npmjs.com/package/dynamoose
Release v2.7.0 · dynamoose/dynamoose · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/dynamoose/dynamoose/releases/tag/v2.7.0

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

981554 Nodejs (npm) Security Update for dynamoose (GHSA-rrqm-p222-8ph2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dynamoosejs	Dynamoose	All	All	All	All
Application	Dynamoosejs	Dynamoose	All	All	All	All
cpe:2.3:a:dynamoosejs:dynamoose:*:*:*:*:node.js:*:*						
cpe:2.3:a:dynamoosejs:dynamoose:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

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

[← Previous ID](#)

[Next ID →](#)

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](#)