



CVE-2022-25948

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-25948
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-22 05:15:00 UTC
Updated	2022-12-30 22:00:00 UTC
Description	The package liquidjs before 10.0.0 are vulnerable to Information Exposure when ownPropertyOnly parameter is set to False

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liquidjs	Liquidjs	All	All	All	All

References

Reference	Source	Link	Tag
leaking JS prototype getter functions in evaluation (eg, .length) · Issue #454 · harttle/liquidjs · GitHub	CONFIRM	github.com	
Information Exposure in liquidjs CVE-2022-25948 Snyk	CONFIRM	security.snyk.io	
feat: `ownPropertyOnly` option to protect prototype, #454 · harttle/liquidjs@7e99efc · GitHub	CONFIRM	github.com	
Google Groups	CONFIRM	groups.google.com	
refactor: change `ownPropertyOnly` default value to `true` · harttle/liquidjs@7eb6216 · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

LEGACY: amit777

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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