



CVE-2022-25887

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-25887
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-30 05:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	The package sanitize-html before 2.7.1 are vulnerable to Regular Expression Denial of Service (ReDoS) due to insecure gl

Risk And Classification

Problem Types: CWE-1333

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apostrophecms	Sanitize-html	All	All	All	All

References

Reference	Source	Link
Regular Expression Denial of Service (ReDoS) in org.webjars.npm:sanitize-html CVE-2022-25887 Snyk	CONFIRM	security.snyk.io
Regular Expression Denial of Service (ReDoS) in sanitize-html CVE-2022-25887 Snyk	CONFIRM	security.snyk.io
Merge pull request #557 from apostrophecms/release-2.7.1 · apostrophecms/sanitize-html@b4682c1 · GitHub	CONFIRM	github.com
Release 2.7.1 by boutell · Pull Request #557 · apostrophecms/sanitize-html · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Nariyoshi Chida of NTT Security Japan

Legacy QID Mappings

[184069](#) Debian Security Update for node-sanitize-html (CVE-2022-25887)

© [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](#)