



CVE-2021-23382

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

Summary

CVE	CVE-2021-23382
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-26 16:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	The package postcss before 8.2.13 are vulnerable to Regular Expression Denial of Service (ReDoS) via getAnnotationURL

Risk And Classification

Problem Types: CWE-1333

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Merge pull request #1567 from yetingli/main · postcss/postcss@2b1d04c · GitHub	MISC	github.com	
Invalid vulnerability	MISC	snyk.io	
Invalid vulnerability	MISC	snyk.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Yeting Li

Legacy QID Mappings

179426 Debian Security Update for node-postcss (CVE-2021-23382)

378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

© [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](#).

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