



CVE-2020-28501

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

Summary

CVE	CVE-2020-28501
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-22 12:15:00 UTC
Updated	2021-03-26 02:39:00 UTC
Description	This affects the package es6-crawler-detect before 3.1.3. No limitation of user agent string length supplied to regex operator

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crawlerdetect Project	Crawlerdetect	All	All	All	All

References

Reference	Source	Link	Tags
sandboxing the module by exx8 · Pull Request #27 · JefferyHus/es6-crawler-detect · GitHub	CONFIRM	github.com	
Regular Expression Denial of Service (ReDoS) in es6-crawler-detect Snyk	CONFIRM	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: Eran Levin

Legacy QID Mappings

[982786](#) Nodejs (npm) Security Update for es6-crawler-detect (GHSA-jxg6-fhwc-9v9c)

© [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](#)