



CVE-2020-5263

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

Summary

CVE	CVE-2020-5263
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-09 16:15:00 UTC
Updated	2020-04-10 13:25:00 UTC
Description	auth0.js (NPM package auth0-js) greater than version 8.0.0 and before version 9.12.3 has a vulnerability. In the case of an

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Auth0	Auth0.js	All	All	All	All

References

Reference	Source	Link	Tags
Information disclosure through error object · Advisory · auth0/auth0.js · GitHub	CONFIRM	github.com	Third Party Advisory
Merge pull request from GHSA-prfq-f66g-43mp · auth0/auth0.js@355ca74 · GitHub	MISC	github.com	Patch, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983125 Nodejs (npm) Security Update for auth0-js (GHSA-prfq-f66g-43mp)

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](#)