



CVE-2020-26288

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

Summary

CVE	CVE-2020-26288
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-30 20:15:00 UTC
Updated	2021-01-04 21:01:00 UTC
Description	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. It is an npm packa

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Parseplatform	Parse-server	All	All	All	All
Application	Parseplatform	Parse-server	All	All	All	All

References

Reference	Source	Link	Tags
parse-server	MISC	www.npmjs.com	Produ
LDAP auth stores password in plain text · Advisory · parse-community/parse-server · GitHub	CONFIRM	github.com	Third
Release 4.5.0 · parse-community/parse-server · GitHub	MISC	github.com	Rele:
Merge pull request from GHSA-4w46-w44m-3jq3 · parse-community/parse-server@da905a3 · GitHub	MISC	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983235](#) Nodejs (npm) Security Update for parse-server (GHSA-4w46-w44m-3jq3)

© [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](#)