Parse Server: LiveQuery protected-field guard bypass via array-like logical operator value

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-34595
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 16:16:34 UTC
Updated	2026-04-01 14:24:02 UTC
Description	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000450000 probability, percentile 0.137700000 (date 2026-04-01)

Problem Types: CWE-843 | CWE-843 CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/S
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Parse-community	Parse-server	affected < 8.6.70	Not specified
CNA	Parse-community	Parse-server	affected >= 9.0.0, < 9.7.0-alpha.18	Not specified

References

Reference	Source	Link	Tags
github.com/parse-community/parse-server/pull/10350	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/commit/f63fd1a3fe0a7c1c5fe809f01...	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/security/advisories/GHSA-mmg8-87...	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/pull/10351	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/commit/ffad0ec6b971ee0dd9545e1bf...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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