



# Parse Server: LiveQuery protected field leak via shared mutable state across concurrent subscribers

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

## Summary

<b>CVE</b>	CVE-2026-34363
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 15:16:18 UTC
<b>Updated</b>	2026-04-01 14:24:02 UTC
<b>Description</b>	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 8.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000850000 probability, percentile 0.247520000 (date 2026-04-01)

**Problem Types:** CWE-362 | CWE-362 CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality **None**

Integrity **None**

Availability **None**

Sub Conf. **None**

Sub Integrity **None**

Sub Availability **None**

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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/MSX/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 < 8.6.65	Not specified
CNA	Parse-community	Parse-server	affected >= 9.0.0, < 9.7.0-alpha.9	Not specified

#### References

Reference	Source	Link	Tags
github.com/parse-community/parse-server/pull/10330	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/commit/5834e29234593addaa0251a85...	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/pull/10331	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/security/advisories/GHSA-m983-v2...	security-advisories@github.com	github.com	
github.com/parse-community/parse-server/commit/776c71c3078e77d38c94937f4...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

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 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](#)**