



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

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

## Summary

<b>CVE</b>	CVE-2026-34595
<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 16:16:34 UTC
<b>Updated</b>	2026-04-02 17:12:56 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 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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000300000 probability, percentile 0.085790000 (date 2026-04-07)

**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/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	5.3	MEDIUM	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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

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/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

Source	Vendor	Product	Version	Reference
CNA	<a href="#">Parse-community</a>	<a href="#">Parse-server</a>	affected < 8.6.70	Not specified
CNA	<a href="#">Parse-community</a>	<a href="#">Parse-server</a>	affected >= 9.0.0, < 9.7.0-alpha.18	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/parse-community/parse-server/pull/10350">github.com/parse-community/parse-server/pull/10350</a>	security-advisories@github.com	<a href="#">github.com</a>	Issue 7
<a href="https://github.com/parse-community/parse-server/commit/f63fd1a3fe0a7c1c5fe809f01...">github.com/parse-community/parse-server/commit/f63fd1a3fe0a7c1c5fe809f01...</a>	security-advisories@github.com	<a href="#">github.com</a>	Patch
<a href="https://github.com/parse-community/parse-server/security/advisories/GHSA-mmg8-87...">github.com/parse-community/parse-server/security/advisories/GHSA-mmg8-87...</a>	security-advisories@github.com	<a href="#">github.com</a>	Patch,
<a href="https://github.com/parse-community/parse-server/pull/10351">github.com/parse-community/parse-server/pull/10351</a>	security-advisories@github.com	<a href="#">github.com</a>	Issue 7
<a href="https://github.com/parse-community/parse-server/commit/ffad0ec6b971ee0dd9545e1bf...">github.com/parse-community/parse-server/commit/ffad0ec6b971ee0dd9545e1bf...</a>	security-advisories@github.com	<a href="#">github.com</a>	Patch
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

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

© [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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)