



# Parse Server has a file upload Content-Type override via extension mismatch

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

## Summary

<b>CVE</b>	CVE-2026-35200
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 20:16:27 UTC
<b>Updated</b>	2026-04-07 18:01:08 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 8.6.73 and

## Risk And Classification

**Primary CVSS:** v4.0 2.1 LOW from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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:** 0.000400000 probability, percentile 0.119330000 (date 2026-04-07)

**Problem Types:** CWE-436 | CWE-436 CWE-436: Interpretation Conflict

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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/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

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/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
CVE	Parseplatform	Parse-server	1.0.0 - 1.0.1	Android, iOS

CNA	<a href="#">Parse-community</a>	<a href="#">Parse-server</a>	affected >= 9.0.0, < 9.7.1-alpha.4	Not specified
CNA	<a href="#">Parse-community</a>	<a href="#">Parse-server</a>	affected < 8.6.73	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/parse-community/parse-server/security/advisories/GHSA-vr5f-2r...">github.com/parse-community/parse-server/security/advisories/GHSA-vr5f-2r...</a>	security-advisories@github.com	<a href="#">github.com</a>	Mitigation,
<a href="https://github.com/parse-community/parse-server/pull/10383">github.com/parse-community/parse-server/pull/10383</a>	security-advisories@github.com	<a href="#">github.com</a>	Issue Track
<a href="https://github.com/parse-community/parse-server/pull/10384">github.com/parse-community/parse-server/pull/10384</a>	security-advisories@github.com	<a href="#">github.com</a>	Issue Track
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical,

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)