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

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-35200
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-06 20:16:27 UTC
Updated	2026-04-07 18:01:08 UTC
Description	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 8.6.73 an

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/MSC:X/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/S
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/S
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/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/MSC: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

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

CNA	Parse-community	Parse-server	affected >= 9.0.0, < 9.7.1-alpha.4	Not specified
CNA	Parse-community	Parse-server	affected < 8.6.73	Not specified

References

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

No vendor comments have been submitted for this CVE.

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