Parse Server: MFA single-use token bypass via concurrent authData login requests

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-34224
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 15:16:18 UTC
Updated	2026-04-02 16:16:23 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 2.1 LOW from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:N/VI:L/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

Problem Types: CWE-367 | CWE-367 CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:N/VI:L/V/
4.0	CNA	DECLARED	2.1	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:N/VI:L/V/
3.1	nvd@nist.gov	Primary	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N
3.1	ADP	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:N/VI:L/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/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 < 8.6.64	Not specified
CNA	Parse-community	Parse-server	affected >= 9.0.0, < 9.7.0-alpha.8	Not specified

References

Reference	Source	Link	Tags
github.com/parse-community/parse-server/pull/10326	security-advisories@github.com	github.com	Issue
github.com/parse-community/parse-server/commit/e7efbebba398ce6abe5b6b6fb...	security-advisories@github.com	github.com	Patch
github.com/parse-community/parse-server/security/advisories/GHSA-w73w-g5...	security-advisories@github.com	github.com	Patch
github.com/parse-community/parse-server/pull/10327	security-advisories@github.com	github.com	Issue
github.com/parse-community/parse-server/commit/661f160edac8daac0486bc944...	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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