multiparty vulnerable to Denial of Service via Prototype Pollution leading to Uncaught Exception

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

Summary

CVE	CVE-2026-8161
State	PUBLISHED
Assigner	openjs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 10:16:48 UTC
Updated	2026-05-12 15:08:22 UTC
Description	multiparty@4.2.3 and lower versions are vulnerable to denial of service via uncaught exception. By sending a multipart/form

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ce714d77-add3-4f53-aff5-83d477b104bb

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

EPSS: 0.000410000 probability, percentile 0.123730000 (date 2026-05-12)

Problem Types: CWE-248 | CWE-1321 | CWE-248 CWE-248: Uncaught Exception | CWE-1321 CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Version	Source	Type	Score	Severity	Vector
3.1	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Multiparty	Multiparty	affected 4.2.3 semver	Not specified
CNA	Multiparty	Multiparty	unaffected 4.3.0 semver	Not specified

References

Reference	Source	Link	Tags
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	cna.openjsf.org	
github.com/pillarjs/multiparty/security/advisories/GHSA-qxch-whhj-8956	ce714d77-add3-4f53-aff5-83d477b104bb	github.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit

CNA: Ser0n-ath (en)

CNA: Sebastian Beltran (en)

CNA: kq5y (en)

CNA: Byambadalai Sumiya (en)

CNA: Blake Embrey (en)

CNA: Ulises Gascón (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**