



# Mastodon has a GET-Based Open Redirect via `'/web/%2F<domain>'`

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

## Summary

<b>CVE</b>	CVE-2026-33868
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 20:16:34 UTC
<b>Updated</b>	2026-03-30 19:14:17 UTC

**Description** Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 4.5.8, 4.4.15, and 4.3.21, an

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-601 | CWE-601 CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	security-advisories@github.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/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	Joinmastodon	Mastodon	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mastodon	Mastodon	affected >= 4.5.0, < 4.5.8	Not specified
CNA	Mastodon	Mastodon	affected >= 4.4.0, < 4.4.15	Not specified
CNA	Mastodon	Mastodon	affected < 4.3.21	Not specified

### References

Reference	Source	Link	Tags
github.com/mastodon/mastodon/security/advisories/GHSA-xqw8-4j56-5hj6	security-advisories@github.com	github.com	Vendor Adviso
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

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.

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