Discourse: Missing post-level authorization allows whisper metadata disclosure

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-32620
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 18:16:50 UTC
Updated	2026-04-01 14:23:37 UTC
Description	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.3, 2026.2.0-latest to befo

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from security-advisories@github.com

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

EPSS: 0.000420000 probability, percentile 0.127200000 (date 2026-04-01)

Problem Types: CWE-200 | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/S
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Discourse	Discourse	affected >= 2026.1.0-latest, < 2026.1.3	Not specified
CNA	Discourse	Discourse	affected >= 2026.2.0-latest, < 2026.2.2	Not specified
CNA	Discourse	Discourse	affected >= 2026.3.0-latest, < 2026.3.0	Not specified

References

Reference	Source	Link	Tags
github.com/discourse/discourse/security/advisories/GHSA-xgg2-vwr6-2c65	security-advisories@github.com	github.com	
github.com/discourse/discourse/commit/bf8dbf6155ae483245d42a0164181bc226...	security-advisories@github.com	github.com	
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.

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