



# Discourse: Missing post-level authorization allows whisper metadata disclosure

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

## Summary

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

## 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/MSX/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/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

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/MSX/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	<a href="#">Discourse</a>	<a href="#">Discourse</a>	affected >= 2026.1.0-latest, < 2026.1.3	Not specified
CNA	<a href="#">Discourse</a>	<a href="#">Discourse</a>	affected >= 2026.2.0-latest, < 2026.2.2	Not specified
CNA	<a href="#">Discourse</a>	<a href="#">Discourse</a>	affected >= 2026.3.0-latest, < 2026.3.0	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://github.com/discourse/discourse/security/advisories/GHSA-xgg2-vwr6-2c65">github.com/discourse/discourse/security/advisories/GHSA-xgg2-vwr6-2c65</a>	security-advisories@github.com	<a href="#">github.com</a>	
<a href="https://github.com/discourse/discourse/commit/bf8dbf6155ae483245d42a0164181bc226...">github.com/discourse/discourse/commit/bf8dbf6155ae483245d42a0164181bc226...</a>	security-advisories@github.com	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canon

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](#).

