



Flarum: Path traversal in LESS parser via theme color settings (incomplete fix for CVE-2023-27577)

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

Summary

CVE	CVE-2026-41887
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 17:16:30 UTC
Updated	2026-05-12 16:45:18 UTC
Description	Flarum is open-source forum software. Prior to versions 1.8.16 and 2.0.0-rc.1, Flarum's patch for CVE-2023-27577 restricte

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from security-advisories@github.com

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

EPSS: 0.000110000 probability, percentile 0.013390000 (date 2026-05-11)

Problem Types: CWE-22 | CWE-918 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Flarum	Framework	affected < 1.8.16	Not specified
CNA	Flarum	Framework	affected >= 2.0.0-beta.1, < 2.0.0-rc.1	Not specified

References

Reference	Source	Link
github.com/Flarum/framework/security/advisories/GHSA-xjvc-pw2r-6878	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.co
github.com/Flarum/framework/releases/tag/v1.8.16	security-advisories@github.com	github.co
github.com/Flarum/framework/releases/tag/v2.0.0-rc.1	security-advisories@github.com	github.co
github.com/Flarum/framework/commit/2d90a1f19f0e46f8c7e1b07c48ba74b5e38f8410	security-advisories@github.com	github.co
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)