This includes the content, date, number and attributes added by other extensions. An attacker only needs the ability to create new posts on the forum to exploit the vulnerability. This works even if new posts require approval. If they have the ability to edit posts, the attack can be performed even more discreetly by using a single post to scan any size of database and hiding the attack post content afterward. The attack allows the leaking of all posts in the forum database, including posts awaiting approval, posts in tags the user has no access to, and private discussions created by other extensions like FriendsOfFlarum Byobu. This also includes non-comment posts like tag changes or renaming events. The discussion payload is not leaked but using the mention HTML payload it's possible to extract the discussion ID of all posts and combine all posts back together into their original discussions even if the discussion title remains unknown. All Flarum versions prior to 1.6.3 are affected. The vulnerability has been fixed and published as flarum/core v1.6.3. As a workaround, user can disable the mentions extension."> "..."> "#p` syntax. The following behavior never changes no matter if the actor should be able to read the mentioned post or not: A URL to the mentioned post is inserted into the actor post HTML, leaking its discussion ID and post number. The `mentionsPosts` relationship included in the `POST /api/posts` and `PATCH /api/posts/` JSON responses leaks the full JSON:API payload of all mentioned posts without any access control. This includes the content, date, number and attributes added by other extensions. An attacker only needs the ability to create new posts on the forum to exploit the vulnerability. This works even if new posts require approval. If they have the ability to edit posts, the attack can be performed even more discreetly by using a single post to scan any size of database and hiding the attack post content afterward. The attack allows the leaking of all posts in the forum database, including posts awaiting approval, posts in tags the user has no access to, and private discussions created by other extensions like FriendsOfFlarum Byobu. This also includes non-comment posts like tag changes or renaming events. The discussion payload is not leaked but using the mention HTML payload it's possible to extract the discussion ID of all posts and combine all posts back together into their original discussions even if the discussion title remains unknown. All Flarum versions prior to 1.6.3 are affected. The vulnerability has been fixed and published as flarum/core v1.6.3. As a workaround, user can disable the mentions extension." />

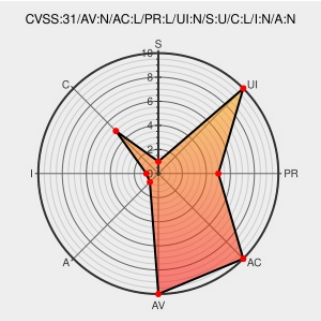
CVE-2023-22487

Published on: Not Yet Published

Last Modified on: 01/19/2023 04:26:00 PM UTC

CVE-2023-22487 - advisory for GHSA-22m9-m3ww-53h3

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Flarum from Flarum contain the following vulnerability:

Flarum is a forum software for building communities. Using the mentions feature provided by the flarum/mentions extension, users can mention any post ID on the forum with the special `@"<username>"#p<id>` syntax. The following behavior never changes no matter if the actor should be able to read the mentioned post or not: A URL to the mentioned post is inserted into the actor post HTML, leaking its discussion ID and post number. The `mentionsPosts` relationship included in the `POST /api/posts` and `PATCH /api/posts/<id>` JSON responses leaks the full JSON:API payload of all mentioned posts without any access control. This includes the content, date, number and attributes added by other extensions. An attacker only needs the ability to create new posts on the forum to exploit the vulnerability. This works even if new posts require approval. If they have the ability to edit posts, the attack can be performed even more discreetly by using a single post to scan any size of database and hiding the attack post content afterward. The attack allows the leaking of all posts in the forum database, including posts awaiting approval, posts in tags the user has no access to, and private discussions created by other extensions like

FriendsOfFlarum Byobu. This also includes non-comment posts like tag changes or renaming events. The discussion payload is not leaked but using the mention HTML payload it's possible to extract the discussion ID of all posts and combine all posts back together into their original discussions even if the discussion title remains unknown. All Flarum versions prior to 1.6.3 are affected. The vulnerability has been fixed and published as flarum/core v1.6.3. As a workaround, user can disable the mentions extension.

CVE-2023-22487 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **flarum** - **framework** version **= < 1.6.3**

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVE References

Description	Tags	Link
Post mentions can be used to read any post on the forum without access control · Advisory · flarum/framework · GitHub	github.com text/html	MISC github.com/flarum/framework/security/advisories/GHSA-22m9-m3ww-53h3
Merge pull request from GHSA-22m9-m3ww-53h3 · flarum/framework@ab1c868 · GitHub	github.com text/html	MISC github.com/flarum/framework/commit/ab1c868b978e8b0d09a5d682c54665dae17d0985

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flarum	Flarum	All	All	All	All

cpe:2.3:a:flarum:flarum:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→