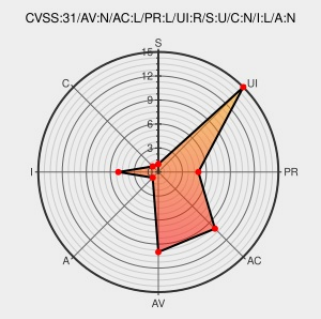
CVE-2023-22489

Published on: Not Yet Published

Last Modified on: 01/23/2023 05:55:00 PM UTC

CVE-2023-22489 - advisory for GHSA-hph3-hv3c-7725

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



Certain versions of Flarum from Flarum contain the following vulnerability:

Flarum is a discussion platform for websites. If the first post of a discussion is permanently deleted but the discussion stays visible, any actor who can view the discussion is able to create a new reply via the REST API, no matter the reply permission or lock status. This includes users that don't have a validated email. Guests cannot successfully create a reply because the API will fail with a 500 error when the user ID 0 is inserted into the database. This happens because when the first post of a discussion is permanently deleted, the `first_post_id` attribute of the discussion becomes `null` which causes access control to be skipped for all new replies. Flarum automatically makes discussions with zero comments invisible so an additional condition for this vulnerability is that the discussion must have at least one approved reply so that `discussions.comment_count` is still above zero after the post deletion. This can open the discussion to uncontrolled spam or just unintentional replies if users still had their tab open before the vulnerable discussion was locked and then post a reply when they shouldn't be able to. In combination with the email notification settings, this could also be used as a way to send unsolicited emails. Versions between `v1.3.0` and `v1.6.3` are impacted. The vulnerability has been fixed and published as flarum/core v1.6.3. All communities running Flarum should upgrade as soon as possible. There are no known workarounds.

CVE-2023-22489 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **flarum** - **framework** version **= >= 1.3.0, < 1.6.3**

CVSS3 Score: 3.5 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

UNCHANGED	NONE	LOW	NONE

CVE References

Description	Tags	Link
Merge pull request from GHSA-hph3-hv3c-7725 · flarum/framework@12f1411 · GitHub	github.com text/html	MISC github.com/flarum/framework/commit/12f14112a0ecd1484d97330b82beb2a145919015
Release v1.6.3 · flarum/framework · GitHub	github.com text/html	MISC github.com/flarum/framework/releases/tag/v1.6.3
Any user including unactivated can reply in public discussions whose first post was permanently deleted · Advisory · flarum/framework · GitHub	github.com text/html	MISC github.com/flarum/framework/security/advisories/GHSA-hph3-hv3c-7725

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→