IDOR in deleting someone else's chat conversation

Moderate **laipz8200** published **GHSA-fxq3-hh7x-c63p** 16 hours ago

Package

Dify

Affected versions

<= 1.9.2

Patched versions

1.13.1

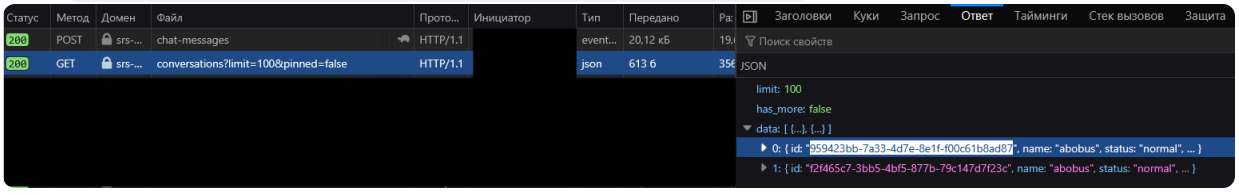
Description

Summary

The method `DELETE /console/api/installed-apps/<appId>/conversations/<conversationId>` has poor authorization checking and allows any Dify-authenticated user to delete someone else's chat history.

Details and PoC

1. Create any application in Dify, type: agent. Set it up and publish this app.
2. Authenticate as user №1 and proceed to chat with that app: https://dify.test/explore/installed/{appId}
3. Click `Start New Chat` on the frontend and write something. Send this message.
4. In DevTools, see a request like `GET /console/api/installed-apps/<appId>/conversations`, which will respond with the `conversationId` and the content of the sent message. I copied GUID №0: `conversationId=959423bb-7a33-4d7e-8e1f-f00c61b8ad87`

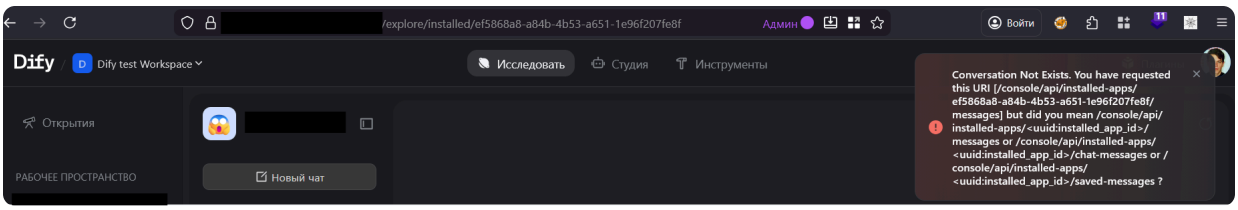


5. On behalf of another authenticated user with any role, send a request of the following type:

```
DELETE /console/api/installed-apps/<appId>/conversations/<conversationId> HTTP/2
Host: dify.test
```

```
Cookie: access_token=<AT>; csrf_token=<CSRF_TOKEN>
X-Csrf-Token: <CSRF_TOKEN>
```

6. Refresh the page and see, that the dialogue has been deleted:



Impact

Any authenticated user with any role can delete any dialog, if he knows GUID of conversation. If GUIDs are leaking somewhere, it's very bad.
This vulnerability leads to loss of integrity.

Severity

Moderate

CVE ID

CVE-2026-34082

Weaknesses

▶ CWE-284

Credits

kast3t Reporter