# Improper Access Control in chocobozzz/peertube



Valid Reported on Dec 31st 2021

## Description

Unauthenticated users can obtain the caption of private videos

## Proof of Concept

1: First, create a private video and upload a caption
2: As an unauthenticated user, logout and visit the

```
/api/v1/videos/1/captions
```

3: The response should return a lazy-static URL

```
{"total":1,"data":[{"language":{"id":"ase","label":"American Sign Language'
```

4: Visit the lazy-static URL and see you can access captions while unauthenticated.

## Impact

This vulnerability is capable of disclosure of captions of private videos to unauthenticated users.

CVE
CVE-2022-0133
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (5.3)

Medium (5.3)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

chocobozzz
@chocobozzz
unranked

This report was seen 362 times.

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

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

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

**chocobozzz** validated this vulnerability a year ago

**haxatron** has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

**chocobozzz** marked this as fixed in **Not released yet** with commit **795212** a year ago

**chocobozzz** has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation