huntr

Server-Side Request Forgery (SSRF) in chocobozzz/peertube

0

✓ Valid Reported on Feb 5th 2022

Description

First of all, Thanks to my friend Haxatron for his excellent report
I read the fix commit, and I found out that the code only Checked the IP addresses and didn't check the domain names that refer to a private IP address

Steps to reproduce

first, set up a local server at `127.0.0.2:8000` and put a media file on it named `1.mp4` .
second, use the following URL to import A video with URL upload when you want to publish a video:

```
http://a.domain.pointing.to.127.0.0.2:8000/1.mp4
```

Impact

You can see that the local server files can be enumerated, and even if there is any media file with a guessable name, it can be leaked through the URL download procedure.

Occurrences

TS video-imports.ts L78

CVE
CVE-2022-0508
(Published)

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity
Medium (6.5)

Chat with us

Visibility

Public

Status

Fixed

Found by

amammad

@amammad

pro

This report was seen 492 times.

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

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

chocobozzz validated this vulnerability 10 months ago

amammad 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 **f33e51** 10 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

video-imports.ts#L78 has been validated ✓

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us