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

0

Valid Reported on Dec 30th 2021

Description

There is an SSRF vulnerability in PeerTube, registered users outside of the external network can issue GET requests into the internal network via the Import With URL option.

Proof of Concept

Setting a Python3 server on 8080

```
python3 -m http.server 8080
```

And importing this URL

```
http://127.0.0.1:8080
```

Will cause a request to be issued to localhost

```
gitpod /workspace/PeerTube $ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
127.0.0.1 - - [30/Dec/2021 10:03:31] "HEAD / HTTP/1.1" 200 -
127.0.0.1 - - [30/Dec/2021 10:03:31] "GET / HTTP/1.1" 200 -
```

Impact

External attackers can port scan and map the internal network. They can also escalate the impact of SSRF to disclose videos stored on webservers on the internal network. For example if a sensitive file is stored in another server http://192.168.0.1/video.mp4, th URL to reveal the video present.

Recommended Fix

The https://www.npmjs.com/package/ipaddr.js/v/1.1.0 package can be used to determine if an IP address is public or private instead of trying to catch all possible private IP addresses.

```
var ipAddr = require('ipaddr.js')

// BAD
console.log(ipAddr.parse("127.0.0.1").range())
console.log(ipAddr.parse("192.168.0.1").range())
console.log(ipAddr.parse("::ffff:7f00:2").range())
console.log(ipAddr.parse("fd12:3456:789a:1::1").range())

// GOOD
console.log(ipAddr.parse("142.251.12.138").range())
```

unicast = good.

```
loopback
private
ipv4Mapped
uniqueLocal
unicast
```

Occurrences

TS import.ts L132L138

References

- Details on SSRF

CVE
CVE-2022-0132
(Published)

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

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

Severity
Medium (4.8)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

chocobozzz
@chocobozzz
unranked

This report was seen 401 times.

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

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron a year ago Researcher

Found a improper access control bug here https://huntr.dev/bounties/80aabdc1-89fe-47b8-87ca-9d68107fc0b4/

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 7b54a8 a year ago

chocobozzz has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

import.ts#L132L138 has been validated ✔

Sign in to join this conversation