Server-Side Request Forgery (SSRF) in janeczku/calibre-web

0

Valid Reported on Dec 20th 2021

Title

Blind SSRF via URL fetch

Summary

`calibre-web` allows external URL fetching in order to upload a book cover. However, instead of external URL it is possible to point to localhost, which will be reached resulting in blind SSRF.

Steps to reproduce

1. As an admin give permissions to upload files and edit books to any staff.
2. As an admin run any server on localhost to see the SSRF.
3. As a malicious staff go to books section -> select any book -> edit metadata -> in the `Fetch Cover from URL` field specify the address of service that you ran as an admin -> save the book.
4. As an admin observe that service on localhost was reached.

PoC:

As a service for PoC I used python simple server - `python -m http.server 1234` . Also you may tunnel `calibre-web` server using `ngrok` - `ngrok http 1234` - to prove that it is exploitable in real environment (I already did, just wanted to make video PoC as short as possible). Video PoC

Impact

This vulnerability is capable of port scanning and even may execute some actions on victim's side in case there are sensitive services on localhost.

References

- https://portswigger.net/web-security/ssrf/blind

CVE
CVE-2022-0339
(Published)

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

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Scaramouche
@scara31
unranked

This report was seen 533 times.

We are processing your report and will contact the janeczku/calibre-web team within 24 hours. a year ago

We have contacted a member of the janeczku/calibre-web team and are waiting to hear back a year ago

We have sent a follow up to the janeczku/calibre-web team. We will try again in 7 days. a year ago

We have sent a second follow up to the janeczku/calibre-web team. We will try again in 10 days. a year ago

We have sent a third and final follow up to the janeczku/calibre-web team. This report is now considered stale. a year ago

janeczku validated this vulnerability 10 months ago

Scaramouche has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

janeczku marked this as fixed in 0.6.16 with commit 3b216b 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

janeczku 10 months ago Maintainer

Accidentally linked the wrong commit, this one is the right one:
https://github.com/janeczku/calibre-web/commit/35f6f4c727c887f8f3607fe3233dbc1980d15020

Scaramouche 10 months ago Researcher

I would also add `0.0.0.0` to a blacklist, it should bypass the restrictions I guess, but overall the fix looks good, thanks!

Sign in to join this conversation