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

0

Valid Reported on Feb 21st 2022

Description

Bypass of this report: https://huntr.dev/bounties/499688c4-6ac4-4047-a868-7922c3eab369/

Proof of Concept

Blacklist does not check for `0.0.0.0`
PAYLOAD: `http://0.0.0.0`
This payload will be resolved to `localhost`

```
>>> import socket
>>> from urllib.parse import urlparse
>>> PAYLOAD = 'http://0.0.0.0'
>>> socket.getaddrinfo(urlparse(PAYLOAD).hostname, 0)[0][4][0]
'0.0.0.0'
```

Impact

SSRF

Occurrences

helper.py L736-L737

CVE
CVE-2022-0766
(Published)

Vulnerability Type

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

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

This report was seen 561 times.

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

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

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

janeczku validated this vulnerability 9 months ago

Rohan Sharma has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Rohan Sharma 9 months ago Researcher

Suggested fix: use ipaddress to implement localhost/internal network ip addresses checks.

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

janeczku marked this as fixed in **0.6.17** with commit **965352** 9 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

helper.py#L736-L737 has been validated ✔

Sign in to join this conversation