huntr

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

0

✓ Valid Reported on Mar 9th 2022

Description

The fix(es) for CVE-2022-0767 & CVE-2022-0766 only address loopback/localhost IP addresses, this is an issue as other internal endpoints may be accessible to an attacker (one of the most popular examples is `169.254.169.254` which is the AWS metadata address)

Proof of Concept

The same as either of the previous reports except the IP address being used should be an internal (but not local/loopback) address (e.g., the aforementioned `169.254.169.254` .

Impact

This vulnerability is capable of allowing attackers to interact with devices (or applications) running on the same network as the targeted server.

Occurrences

helper.py L734

```
if ip.startswith("127.") or ip.startswith('::ffff:7f') or ip == "::1"
    ...
```

Chat with us

CVE

CVE-2022-0990
(Published)

Vulnerability Type

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

Severity
Critical (9.3)

Visibility
Public

Status
Fixed

Found by

Michael Rowley

@michaellrowley

pro ⌄

This report was seen 438 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.
8 months ago

janeczku validated this vulnerability 8 months ago

Michael Rowley has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

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

We have sent a second fix follow up to the **janeczku/calibre-web** team. We
days. 8 months ago

Chat with us

janeczku marked this as fixed in 0.6.18 with commit 4545f4 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

helper.py#L734 has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us