Improper Access Control in janeczku/calibre-web

Valid Reported on Jan 23rd 2022

Description

With default settings, low-level users will not have permission to read name of private shelf (shelf create by another user and not in public mode). However, due to incorrect HTML render, 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 "test2" with default permissions (only "Show *" permissions).
Step 2: Using admin account and create private shelf. Get id of this shelf.
Step 3: Login as test1 and go to http://hostname:8083/shelf/order/:id. Attacker will get name of private shelf. id for this attack can get via brute-force.
PoC: https://drive.google.com/file/d/10tbKwfXlNXMgPEa0i4pPZ1-wW2ovUpsM

Root-cause

In line 380 (https://github.com/janeczku/calibre-web/blob/master/cps/shelf.py#L380), server will check view permission of user and query book for shelf. However, if user doesn't have view permission, server continues to render HTML containing shelf.name instead of showing error messages and redirect. This leads to disclose name of private shelf.

Impact

Low-level user can read name of all private shelves.

CVE
CVE-2022-0405
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

nhiephon
@nhiephon
master

This report was seen 365 times.

We are processing your report and will contact the **janeczku/calibre-web** team within 24 hours. 10 months ago

nhiephon modified the report 10 months ago

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

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

janeczku marked this as fixed in 0.6.16 with commit 3b216b 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation