huntr

Improper Access Control in janeczku/calibre-web

0

✓ Valid Reported on Jan 17th 2022

Description

With default settings, low-level users will not have permission to create new shelf with public mode. However, due to incorrect checking, the function does not work as intended.

Steps To Reproduce

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: Login as test1 and create new shelf, intercept request, add "is_public=off" to POST data. test1 can create public shelf without "Public Shelf" permission.
PoC: https://drive.google.com/file/d/17KuxINz7JYPy8FfIvcPViUc0GT4ZHxOl

Root-cause

In line 248 (https://github.com/janeczku/calibre-web/blob/01090169a795342626412955cd0aefea11ad4a2a/cps/shelf.py#L248), server will check if user without "Public shelf" permission add "is_public=on" in create request and return error. However, in line 251, server only check the existence of "is_public" but not check the value again. Attacker can pass a value different "on" to pass this check.

Impact

Low-level user without "Public Shelf" permission can create public shelf. This can leads to malicious content being shared publicly.

CVE
CVE-2022-0273
(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 367 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

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

janeczku validated this vulnerability 10 months ago

nhiephon has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

janeczku marked this as fixed in **0.6.16** with commit **0c0313** 10 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation

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