huntr

Stored XSS via File Upload in star7th/showdoc in star7th/showdoc

0

✓ Valid Reported on Mar 14th 2022

Description

Stored XSS via uploading file in .properties format.

Proof of Concept

```
filename="test.properties"

<script>alert(1)</script>
```

Steps to Reproduce

Login into showdoc.com.cn.
Navigate to file library (https://www.showdoc.com.cn/attachment/index)
In the File Library page, click the Upload button and choose the test.properties file.
After uploading the file, click on the check button to open that file in a new tab.
XSS will trigger when the attachment is opened in a new tab.

POC URL:

`https://img.showdoc.cc/622f467833127_622f467833120.properties?e=1647269010&token=-YdeH6WvESHZKz-yUzWjO-uVV6A7oVrCN3UXi48F:o4Avvyq1nJSSadhWuytWRYg6K1Q=`

Impact:

An attacker can perform social engineering on users by redirecting them from a real website to a fake one. a hacker can steal their cookies etc.

CVE

CVE-2022-0966
(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.4)

Visibility
Public

Status
Fixed

Found by

Akshay Ravi
@akshayravic09yc47
pro

Fixed by

star7th
@star7th
unranked

This report was seen 573 times.

We are processing your report and will contact the **star7th/showdoc** team within 24 hours.
8 months ago

Akshay Ravi modified the report 8 months ago

Akshay Ravi modified the report 8 months ago

star7th validated this vulnerability 8 months ago

Akshay Ravi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

star7th marked this as fixed in 2.4.10 with commit 3caa32 8 months ago star7th marked this as fixed in 2.4.0 with commit 5eda52 8 months ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation