Cookie is persisting in the browser which leads to Session Fixation in ikus060/rdiffweb

1

Valid Reported on Sep 18th 2022

Description

After logging in and logging out, the application continues to use the preauthentication cookies. The cookies are same after closing the browser and after password change .And also same cookies are reassigning for another user's login which can leads to session fixation.

Proof of Concept

Checklist

[ ] Check cookie before authentication
[ ] Check cookie after guest user authentication
[ ] Check cookie after admin user authentication
[ ] Check cookie after logout
[ ] Check cookie after closing the browser

```
POC : https://drive.google.com/file/d/1nur3xAzgPJB4mgEAyQANVr4f2sOm4HmW/vie
```

Impact

An attacker can gain unauthorized access to the account of users who are using the same browser as long as a single session cookie persists on that browser once the attacker obtains a session cookie through another attack.

References

- https://livebook.manning.com/book/practical-python-security/chapter-7/

CVE
CVE-2022-3269
(Published)

Vulnerability Type
CWE-384: Session Fixation

Severity
Medium (6.4)

Registry
Pypi

Affected Version
2.4.4 and below

Visibility
Public

Status
Fixed

Found by

Ambadi MP
@ciph0x01
legend

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 816 times.

We are processing your report and will contact the **ikus060/rdiffweb** team within 24 hours.
2 months ago

Ambadi MP modified the report 2 months ago

We have contacted a member of the **ikus060/rdiffweb** team and are waiting
2 months ago

Chat with us

Patrik Dufresne validated this vulnerability 2 months ago

Ambadi MP has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Patrik Dufresne 2 months ago Maintainer

@admin May you plz assign a CVE

Thanks

Jamie Slome 2 months ago Admin

Sorted :)

Patrik Dufresne marked this as fixed in 2.4.7 with commit 39e7dc 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team