Session does not expire on password reset in ikus060/rdiffweb

1

Valid Reported on Sep 29th 2022

Description

On changing password both session using which user changes password and old sessions in any other browser or device does not expire and remains active

Proof of Concept

```
1.Go to https://rdiffweb-dev.ikus-soft.com/login/ and login into same accou
2.From Browser B  change password associated with your account
3.Notice that Session on Browser A will remain active and does not expire.



# Impact

All active sessions must expire on password change to revoke access from a
```

References

- Hackerone Report

CVE
CVE-2022-3362
(Published)

Vulnerability Type

CWE-613: Insufficient Session Expiration

Severity
Medium (6.1)

Registry
Pypi

Affected Version
2.4.9

Visibility
Public

Status
Fixed

Found by

nehalr777
@nehalr777
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 344 times.

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

Patrik Dufresne assigned a CVE to this report 2 months ago

Patrik Dufresne validated this vulnerability 2 months ago

nehalr777 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **ikus060/rdiffweb** team. We will try again in 7 days.
2 months ago

We have sent a second fix follow up to the **ikus060/rdiffweb** team. We will try again in 10 days.
2 months ago

We have sent a third and final fix follow up to the **ikus060/rdiffweb** team. This report is now considered stale. a month ago

Patrik Dufresne marked this as fixed in **2.5.0** with commit **6efb99** 12 days ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability has been assigned a CVE ✔

Patrik Dufresne published this vulnerability 12 days ago

Sign in to join this conversation