Cross Site Request Forgery in Admin area leads to deletion of repositories and users in ikus060/rdiffweb

0

Valid Reported on Sep 16th 2022

Description

Server accepts the GET request for deleting repositories and users which can lead to CSRF attack on repositories'.

Proof of Concept

Open the below URL after logging in to the admin account in demo site.
For deleting Repository : Replace "replace-here" with a repo name

```
https://rdiffweb-demo.ikus-soft.com/delete/admin/replace-here?action=&confi
```

For deleting User

```
https://rdiffweb-demo.ikus-soft.com/admin/users?action=delete&username=u
```

Impact

Deletion of repositories and users

Occurrences

page_delete.py L64-L81

References

- https://guides.codepath.com/websecurity/Cross-Site-Request-Forgery#:~:text=the%20user's%20browser.-,CSRF%20GET%20Request,or%20in%20a%20phishing%20email.

CVE
CVE-2022-3232
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (6.5)

Registry
Pypi

Affected Version
2.4.3 and below

Visibility
Public

Status
Fixed

Found by

Ambadi MP
@ciph0x01
legend

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 2,237 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

Ambadi MP modified the report 2 months ago

Patrik Dufresne validated this vulnerability 2 months ago

I confirm the vulnerability.

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 could we get an CVE for this repport.
Thanks

Jamie Slome 2 months ago Admin

Sorted :)

Patrik Dufresne marked this as fixed in 2.4.5 with commit 422791 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

page_delete.py#L64-L81 has been validated ✔

Sign in to join this conversation