

CSRF leads to disabling notifications in users profile in ikus060/rdiffweb

0



Valid

Reported on Sep 16th 2022

Description

Periodic updates of repositories were sent as notifications to the user's email and here GET request sent to the server for modifying repository notifications settings is accepted by the server, which can lead to disabling notifications through a CSRF attack.

Proof of Concept

Replace repos with valid repo names

```
https://rdiffweb-demo.ikus-soft.com/prefs/notification?repo1%2FC=0&repo2=0&
```



example:

```
https://rdiffweb-demo.ikus-soft.com/prefs/notification?MyWindowsLaptop%2FC=
```



Impact

Repository notifications sent to user's email will be disabled.

References

- <https://guides.codepath.com/websecurity/Cross-Site-Request-Forgery>

[Chat with us](#)

(Published)

Vulnerability Type

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

Severity

Medium (4.3)

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 705 times.

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

2 months ago

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

Chat with us

Patrik Dufresne [2 months ago](#)

Maintainer

@admin could to assign a CVE to this repport

Jamie Slome [2 months ago](#)

Admin

Done :)

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

Patrik Dufresne marked this as fixed in **2.4.6** with commit **18a5aa** [2 months ago](#)

Patrik Dufresne has been awarded the fix bounty 

This vulnerability will not receive a CVE 

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us

[terms](#)

[privacy policy](#)

[Chat with us](#)