CSRF to change the email id in ikus060/rdiffweb

1

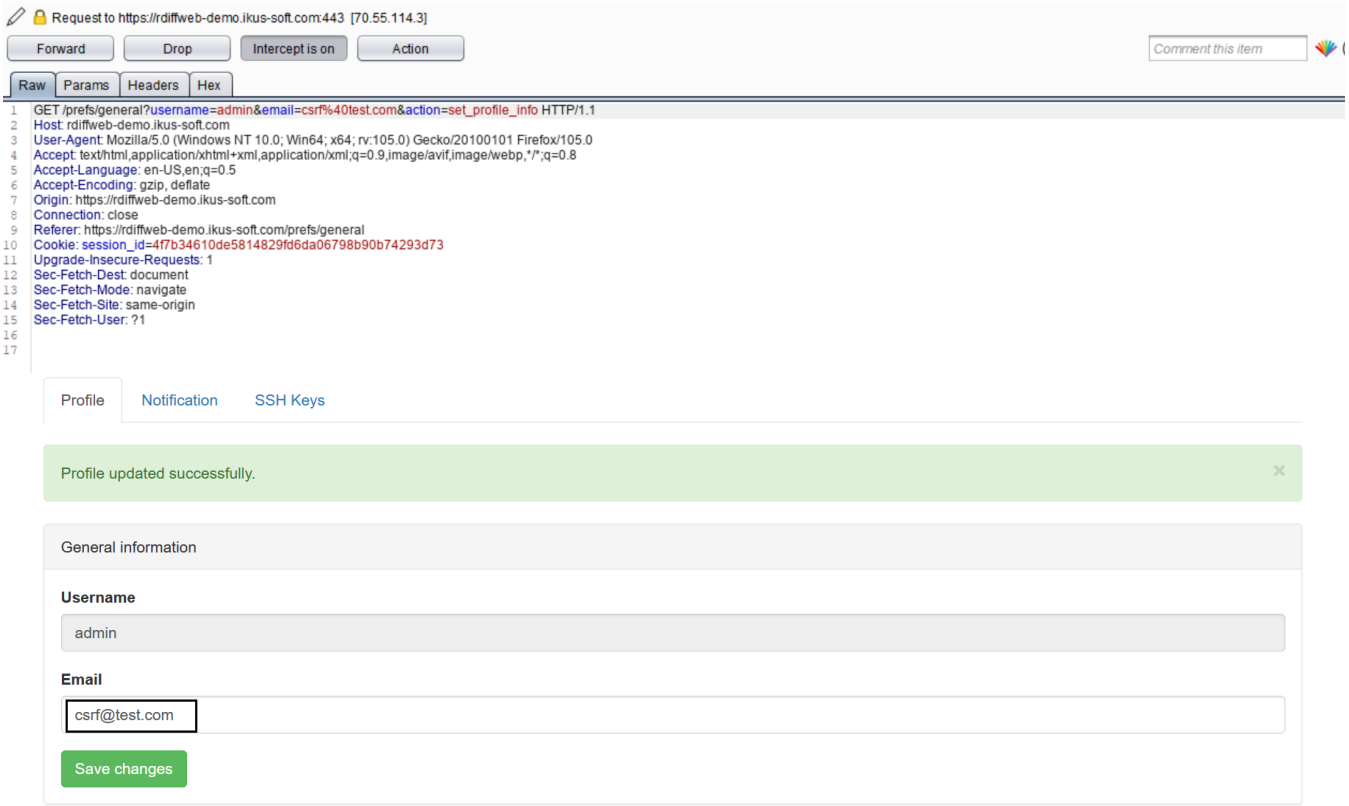
Valid Reported on Sep 21st 2022

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.



Impact

This could change the email ID of the user.

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 [illegible] earlier.

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

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