The settings of repositories is vulnerable to CSRF in ikus060/rdiffweb

0

Valid Reported on Sep 19th 2022

Description

The malicious user can change the settings of repository by sending the URL to the victim.

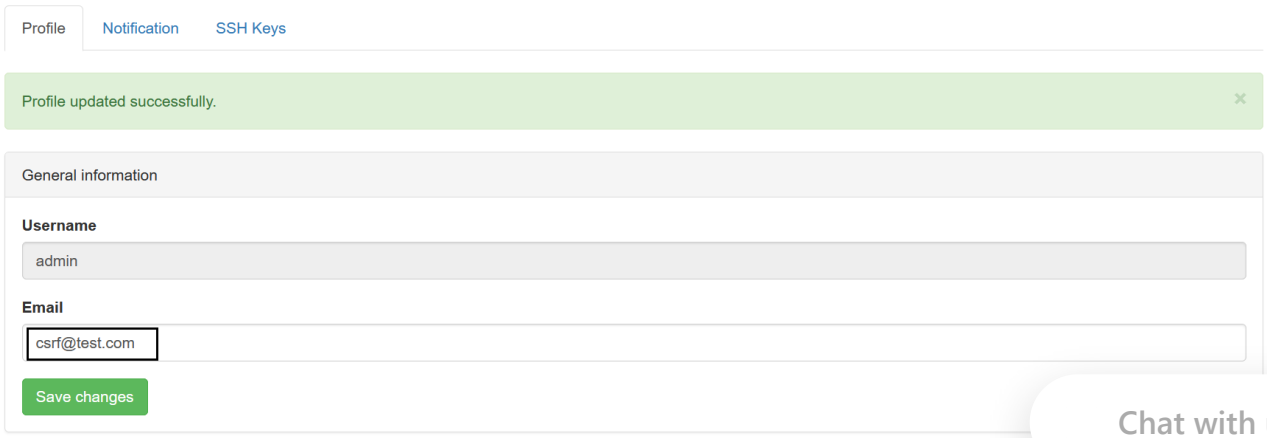
Proof of Concept

1.Login into the application https://rdiffweb-demo.ikus-soft.com/settings/admin/test-encoding .

2.Go to test-encoding.

3.Check that the value of remove older is forever.

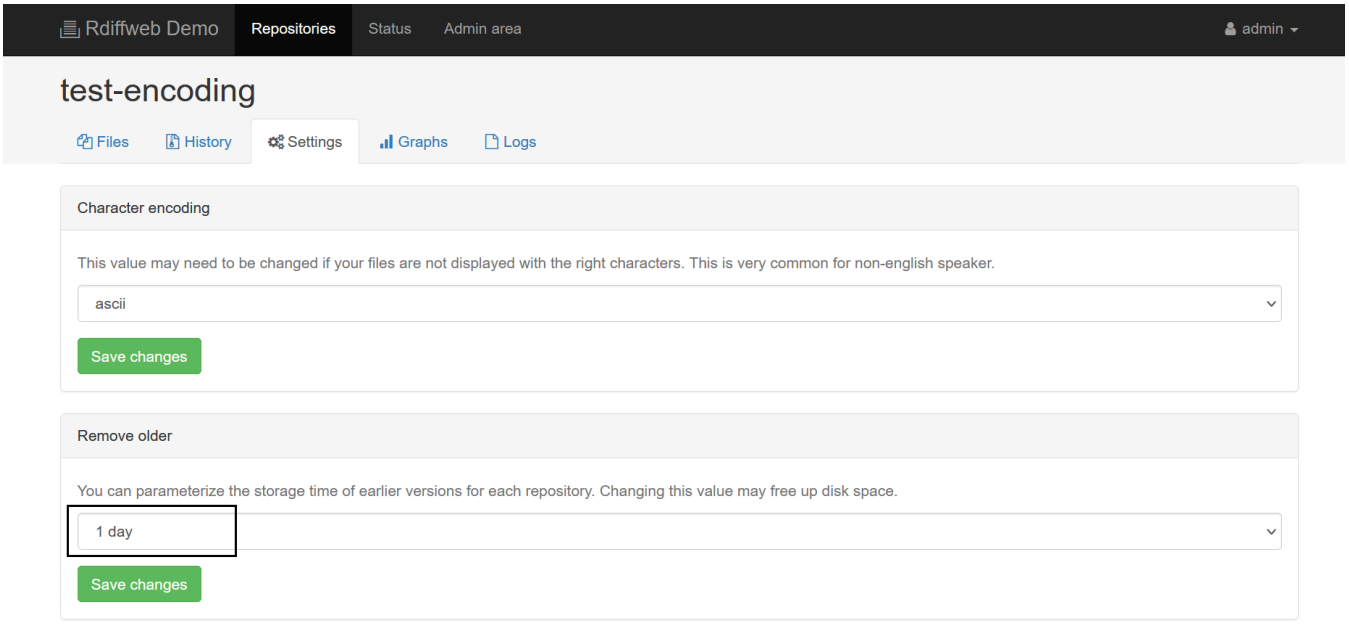
4.Open the URL https://rdiffweb-demo.ikus-soft.com/settings/admin/test-encoding?keepdays=1 .



5.Refresh the page.

6.The setting is updated

6. The setting is updated.



Impact

A malicious user can change the setting of repository.

CVE
CVE-2022-3267
(Published)

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

Severity
Medium (6.8)

Registry
Npm

Affected Version
2.5

Visibility
Public

Status
Fixed

Found by
irfansayyed-github

irfansayyed-github

@irfansayyed-github

master

Fixed by

Patrik Dufresne

@ikus060

unranked

This report was seen 733 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

irfansayyed-github has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

irfansayyed-github 2 months ago — Researcher

@admin Could we get a CVE for this?

Jamie Slome 2 months ago — Admin

Sure, once we get the go-ahead from the maintainer, we can assign and publish a CVE for you :)

Patrik Dufresne marked this as fixed in **2.4.6** with commit **20fc0d** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

irfansayyed-github 2 months ago — Researcher

Hi Maintainer,

Could you reply so that @admin can provide the CVE.

irfansayyed-github 2 months ago Researcher

@admin could you check if we get a CVE.

Patrik Dufresne 2 months ago Maintainer

@admin you may assign a CVE for this report.

Jamie Slome 2 months ago Admin

Sorted :)

> Sign in to join this conversation

terms

privacy policy

Chat with us