huntr

Attacker is able to bypass 2FA verification during 2FA disable due to application logic flaw in ikus060/rdiffweb

1

✓ Valid Reported on Sep 29th 2022

Description

An attacker is able to bypass 2FA verification during 2FA disable function of user and restrict user from accessing his account due to a application logic flaw

Proof of Concept

```
First of all let us consider a scenario where a user has left his account o

1) Go to https://rdiffweb-dev.ikus-soft.com/prefs/mfa , click on disable 2F
2) Lets dive into an application logic flaw.
3) Attacker will go to https://rdiffweb-dev.ikus-soft.com/prefs/general cha
4) He will go back to https://rdiffweb-dev.ikus-soft.com/prefs/mfa and now 
5) As the email associated with the account is attackers email , he will re
6) He can go ahead and disable 2FA now.

POC:
https://drive.google.com/file/d/1iA_JSlhwCLt54IIpRHx2Ey9yt1Sltchq/view?usp=


# Impact

Attacker is able to disable users 2FA , allowing the reduce component secur
```

CVE
CVE-2022-4018
(Published)

Chat with us

Vulnerability Type
CWE-306: Missing Authentication for Critical Function

Severity
Medium (6.1)

Registry
Pypi

Affected Version
2.5.0a3

Visibility
Public

Status
Fixed

Found by

nehalr777
@nehalr777
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 317 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

Would say it's a duplicate of this one: No password confirmation on sensitive action like email change

Basically, the vulnerability in this report is letting the attacker change the em
password verification.

Chat with us

At least, the user get notify of the email address being changed

At least, the user get notify of the email address being changed.

nehalr777 2 months ago Researcher

Let us put a good fix forward:
This can be fixed by implementing password for 2FA feature as well , where it needs both the confirmation code and password as well to disable 2FA.

This way even though attacker has changed the email associated with the account, he won't be able to tamper the 2FA related security implementation

nehalr777 2 months ago Researcher

@maintainer hello sir , what is your opinion on this issue?

Patrik Dufresne validated this vulnerability 2 months ago

@nehalr777 Than change the vulnerability type for "CWE-306: Missing Authentication for Critical Function"

nehalr777 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

nehalr777 2 months ago Researcher

@admin , could you please change vulnerablity type to "CWE-306: Missing Authentication for Critical Function" ?

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

We have sent a second fix follow up to the **ikus060/rdiffweb** team. We will try again in 10 days.
2 months ago

Ben Harvie a month ago

The CWE number has been updated as requested:)

Chat with us

Patrik Dufresne marked this as fixed in **2.5.0a6** with commit **f2a32f** a month ago

Patrik Dufresne has been awarded the fix bounty ✓

This vulnerability has been assigned a CVE ✓

Patrik Dufresne published this vulnerability 12 days ago

Sign in to join this conversation