Weak password policy : Old password can be set as new password in ikus060/rdiffweb

3

Valid Reported on Sep 30th 2022

Description

Rdiffweb has a weak password implementation , where a new password set by the user can be same to the old password

Proof of Concept

Go to https://rdiffweb-demo.ikus-soft.com/prefs/general end point
Change your password
Set your new password similar to old password you will notice that the same password is accepted by the application

Impact

Password changes in the Rdiffweb application would usually happen for one of three reasons: The user has forgotten their password and needs to reset it to a known value. In this case, reuse of the same password is unlikely. 2)The user is aware (or suspects) that their password is known to someone else and wants to reset it to a new value that is known only to them. In this case, the user would be motivated to choose a new password, although it's possible that they could reuse the same password in error. 3)An administrator is aware (or suspects) that the user's password is known to someone else and wants to reset it to a new value that is known only to the user. In this case, the user might be less motivated to choose a new password and password reuse is more likely. However, given the risks of phishing and the importance of ensuring a password reset, it's also likely the administrator would communicate
At the same time, considering the likely human behaviour in each case (and that an attacker would need to combine it with another vulnerability or phishing in order to gain or retain access to a legitimate user's account), the likelihood of successful exploitation of this vulnerability is relatively low.

References

- Hackerone Report

CVE
CVE-2022-3376
(Published)

Vulnerability Type
CWE-521: Weak Password Requirements

Severity
Low (3.5)

Registry
Pypi

Affected Version
2.4.9

Visibility
Public

Status
Fixed

Found by

nehalr777
@nehalr777
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 883 times.

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

Patrik Dufresne 2 months ago

@nehalr777 plz change the version for 2.4.9

Patrik Dufresne assigned a CVE to this report 2 months ago

nehalr777 modified the report 2 months ago

nehalr777 2 months ago Researcher

Done

Patrik Dufresne validated this vulnerability 2 months ago

nehalr777 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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 **2.5.0a4** with commit **2ffc2a** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation