No rate limit on old password parameter allows attacker to bruteforce the existing password and set a new password in ikus060/rdiffweb

4

Valid Reported on Sep 22nd 2022

Description

There is no rate limit on the password change feature on https://rdiffweb-demo.ikus-soft.com/prefs/general# which allows an attacker to bruteforce the old password and set a new password for the account

Proof of Concept

Go to https://rdiffweb-demo.ikus-soft.com/prefs/general#
Here you will see a password change feature
In the "old password" field enter any random string and in the "new password" and "confirm new password" field set the new password for the victim account
Capture the request using burpsuite and perform a bruteforce attack on the old password field
Due to the absence of rate limit on this endpoint an attacker can easily change the password of victim account
Attack Scenario: Let us consider a situation in which a victim is using a public device , in a library or cafe and forgets to log out of his account and an attacker gets access to this device .

Impact

Attacker can perform a bruteforce attack to change the password of the account hence resulting in a full account takeover issue

Occurrences

page_pref_general.py L56-L84

References

- Hackerone Report

CVE
CVE-2022-3273
(Published)

Vulnerability Type
CWE-770: Allocation of Resources Without Limits or Throttling

Severity
Low (3.6)

Registry
Other

Affected Version
2.4.6

Visibility
Public

Status
Fixed

Found by

nehalr777
@nehalr777
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 835 times.

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

Patrik Dufresne assigned a CVE to this report 2 months ago

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

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

Patrik Dufresne marked this as fixed in 2.5.0a4 with commit b5e3bb 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

page_pref_general.py#L56-L84 has been validated ✔

Sign in to join this conversation