Password can be set extremely weak in ikus060/rdiffweb

0

Valid Reported on Sep 9th 2022

Description

In this scenario, I use the demo website. It allows us to add more user to test. With password, we can set it 1 (Or any charater). There is no policy for password or no password checking. Moreover, it also allows us to change password and the new password also can be set with password.

Proof of Concept

Access to the demo website and login as an admin. Add user with password 1 or any charater (short, weak) Try to login with the new user and it succeed.
With normal user, login and try to change password function, it also succeed.

Impact

Be able to get all user's accounts with weak password by bruteforce attack.

CVE
CVE-2022-3179
(Published)

Vulnerability Type
CWE-521: Weak Password Requirements

Severity
High (7.1)

Registry
Other

Affected Version
2.4.1

Visibility
Public

Status
Fixed

Found by

Chuu
@uonghoangminhchau
amateur

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 824 times.

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

Chuu modified the report 3 months ago

Chuu modified the report 3 months ago

Patrik Dufresne validated this vulnerability 3 months ago

Chuu has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chuu 3 months ago Researcher

thank you

Patrik Dufresne 2 months ago

@chuu The affected version is wrong It should be 2.4.1

Patrik Dufresne 2 months ago Maintainer

@admin Is it possible to get a CVE ID ?

Jamie Slome 2 months ago Admin

Updated affected version and sorted a CVE for this report :)

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 **2.4.2** with commit **233bef** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

terms

privacy policy

Chat with us