Password Can be set to very weak in ikus060/minarca

1

Valid Reported on Sep 13th 2022

Description

For testing the issue, I have used the demo website. In edit user profile section we can set New Password to 1 (Or any character). 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 weak password.

Proof of Concept

Access to the demo website and login as an admin. Edit user with New password 1 or any character (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

Attacker will able to get all user's accounts with weak password using bruiteforce attack.

CVE
CVE-2022-3268
(Published)

Vulnerability Type
CWE-521: Weak Password Requirements

Severity
Critical (9.8)

Registry
Other

Affected Version
4.2.0

Visibility
Public

Status
Fixed

Found by

Vanilla
@vanilla-ctrl
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 2,942 times.

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

Patrik Dufresne validated this vulnerability 2 months ago

This vulnerability is valid. Was reported on Rdiffweb project.

Minarca will get fixed, whenever I upgrade Rdiffweb version embedded in Minarca.

Vanilla has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Vanilla 2 months ago Researcher

Hi @patrik,
Thank you for the update.

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

Vanilla 2 months ago Researcher

Hi @admin,
can we proceed for the CVE ?

Jamie Slome 2 months ago Admin

Happy to once we get the go-ahead from the maintainer 👍

Patrik Dufresne marked this as fixed in 4.2.2 with commit 7b5c7e 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Patrik Dufresne 2 months ago Maintainer

@admin You may assign a CVE to this report

Jamie Slome 2 months ago Admin

Sorted :)

Sign in to join this conversation