Bypassing application logic to set a blank password in ikus060/rdiffweb

2

Valid Reported on Sep 26th 2022

Description

As you many observe that rdiffweb strictly has a password policy where it prompts out that the password should be between 8 and 128 characters . But the application does not filter blank spaces used in a password

Proof of Concept

```
1) Go to https://rdiffweb-demo.ikus-soft.com/prefs/general
2) Change the password . Old password - admin123 and set the new password a
3) You can see that the application accepts blank spaces in a password and
```

```
# Impact

This way user will be able to set a blank password bypassing the applicatic
```

Occurrences

prefs_general.html L1-L30

References

Chat with us

- Hackerone

CVE
CVE-2022-3326
(Published)

Vulnerability Type
CWE-521: Weak Password Requirements

Severity
Medium (5.4)

Registry
Pypi

Affected Version
2.4.6

Visibility
Public

Status
Fixed

Found by

nehalr777
@nehalr777
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 825 times.

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

Patrik Dufresne 2 months ago

Chat with us

I might consider adding a password entropy requirement. But python library are not readily available in Debian to calculate that.

Something like this :https://ritcyberselfdefense.wordpress.com/2011/09/24/how-to-calculate-password-entropy/

Patrik Dufresne 2 months ago Maintainer

Maybe zxcvbn ?

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

nehalr777 2 months ago Researcher

Hello sir , Thank you for the quick response.
Here is an example
https://github.com/WeblateOrg/weblate/commit/708712e8fb5d990956f695023f0213acd99676ef

nehalr777 2 months ago Researcher

Oh yes! https://ritcyberselfdefense.wordpress.com/2011/09/24/how-to-calculate-password-entropy/

Works :). It's indeed a pretty good idea .

Patrik Dufresne marked this as fixed in 2.4.9 with commit ee98e5 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

prefs_general.html#L1-L30 has been validated ✔

Chat with us

Sign in to join this conversation

2022 © 418sec

Chat with us