huntr

Weak Password Policy in polonel/trudesk

0

✔ **Valid**   Reported on May 17th 2022

Description

I would like to let you know about the password management issue.

Proof of Concept

1- Go to your Profile or https://docker.trudesk.io/profile
2- Give a password as simple as 12345678.
You can see you will be password has been changed and there is no strong enforcement.

Impact

This password can easily be cracked using dictionary attack

Fix:

Use complex password management.

References

- https://nvd.nist.gov/vuln/detail/CVE-2019-14833

CVE
CVE-2022-1775
(Published)

Vulnerability Type
CWE-521: Weak Password Requirements

Severity
High (8.4)

Registry
Other

Chat with us

Affected Version
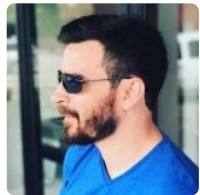*

Visibility
Public

Status
Fixed

Found by

Vishal Vishwakarma
@vishalvishw10
pro ⌄

Fixed by

Chris Brame
@polonel
unranked ⌄

We are processing your report and will contact the **polonel/trudesk** team within 24 hours.
6 months ago

Chris Brame assigned a CVE to this report   6 months ago

Chris Brame validated this vulnerability   6 months ago

This has been fixed in v1.2.2. I will update this report once it has been released.

Vishal Vishwakarma has been awarded the disclosure bounty   ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chris Brame marked this as fixed in **1.2.2** with commit **13dd6c**   6 months ago

Chat with us

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us