huntr

# Allowing long password leads to denial of service in polonel/trudesk in polonel/trudesk

0

✓ Valid Reported on May 15th 2022

Description The trudesk application allows to sending a very long password (10000000 characters) it's possible to cause a denial of service attack on the server. This may lead to the website becoming unavailable or unresponsive. Usually, this problem is caused by a vulnerable password hashing implementation. When a long password is sent, the password hashing process will result in CPU and memory exhaustion.

## Proof of Concept

1.Go to https://docker.trudesk.io/profile paste the payload in Password parameter
2.Copy the payload from this link:- https://drive.google.com/file/d/1E3iqSQE4-t4dXpWQrDPHY7OcspHxYvYE/view?usp=sharing and paste on Password parameter
3.You will see that the application allows long password this can leads to Dos and can exploit as DDos

## Video POC :- https://drive.google.com/file/d/1d_QV79hBqGN6GHSt5VLiranA6hO2q2W_/view?usp=sharing

## Impact

This vulnerability can be abused by doing a DDoS attack for which genuine users will not able to access resources/applications.

## References

- Drupal CVE-2014-9016

CVE
CVE-2022-1728
(Published)

Chat with us

Vulnerability Type
CWE-190: Integer Overflow or Wraparound

Severity
High (7.6)

Registry
Other

Affected Version
<= 1.2.0

Visibility
Public

Status
Fixed

Found by

Vishal Vishwakarma
@vishalvishw10
pro

This report was seen 566 times.

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

Chris Brame validated this vulnerability 6 months ago

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 **e836d0** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Chat with us

Vishal 6 months ago Researcher

@admin can you please assigned this as cve

Jamie Slome 6 months ago Admin

Sorted 👍

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