

The trudesk application allows large characters to insert in the input field "Name" which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request. in polonel / trudesk in polonel/trudesk



Reported on May 16th 2022

Proof of Concept

1 - Go to Profile or <https://docker.trudesk.io/profile>

2 - and fill name input field with huge characters

Payload :- <https://drive.google.com/file/d/17-SH8ZaTqBTQGugpbh2SQtTKnJOL9NIK/view?usp=sharing>

Video POC :-

https://drive.google.com/file/d/1LYSRwVI6hAS_1Q1cYJNYkBgH8YNEBk_Y/view?usp=sharing

Screenshot of POC -:

<https://drive.google.com/file/d/1jKOLbBVq2SOD20bCvvXirOf-5mtsvaEC/view?usp=sharing>

Impact

It can leads to denial of service attack

References

- <https://huntr.dev/bounties/97e36678-11cf-42c6-889c-892d415d9f9e/>
- <https://huntr.dev/bounties/cdf00e14-38a7-4b6b-9bb4-3a71bf24e436/>

(Published)

Vulnerability Type

CWE-190: Integer Overflow or Wraparound

Severity

High (8.4)

Registry

Rubygems

Affected Version

*

Visibility

Public

Status

Fixed

Found by

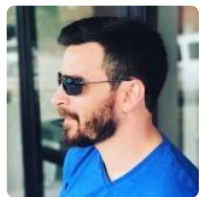


Vishal Vishwakarma

@vishalvishw10

pro ▼

Fixed by



Chris Brame

@polonel

unranked ▼

This report was seen 510 times.

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

6 months ago

A **polonel/trudesk** maintainer has acknowledged this report 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

Chat with us

The researcher's credibility has increased: +7

Chris Brame [6 months ago](#)

Maintainer

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

Vishal [6 months ago](#)

Researcher

@admin can you please assigned as cve

Jamie Slome [6 months ago](#)

Admin

Sorted 👍

We have sent a fix follow up to the **polonel/trudesk** team. We will try again in 7 days.
6 months ago

Chris Brame marked this as fixed in 1.2.2 with commit **e836d0** 6 months ago

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

[hacktivity](#)

[about](#)

[leaderboard](#)

[team](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)