huntr

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

0

✓ Valid Reported on May 14th 2022

POC:

go to signup form: `http://127.0.0.1:8118/signup`
Fill the Full Name input field with huge characters(more than lakhs or crores)
After created the account, check the admin panel: `http://127.0.0.1:8118/accounts` , go to Accounts --> customers
The admin panel will be flooded with our payload

POC Screenshot:

```
https://ibb.co/2Nvj908
```

POC video:

```
https://www.mediafire.com/file/vng5aufoydb6hl5/trudesk-poc.mov/file
```

Impact

It can leads to Senial of service attack

References

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

CVE
CVE-2022-1718
(Published)

Vulnerability Type
CWE-190: Integer Overflow or Wraparound

Severity
High (7.2)

Registry
Other

Affected Version
<= 1.2.0

Visibility
Public

Status
Fixed

Found by

Akshay Ravi
@akshayravic09yc47
pro

Fixed by

Chris Brame
@polonel
unranked

This report was seen 523 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 assigned a CVE to this report 6 months ago

Chris Brame validated this vulnerability 6 months ago

Akshay Ravi has been awarded the disclosure bounty ✓

Chat with us

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 **87e231** 6 months ago

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