Allocation of Resources Without Limits in in polonel/trudesk

0

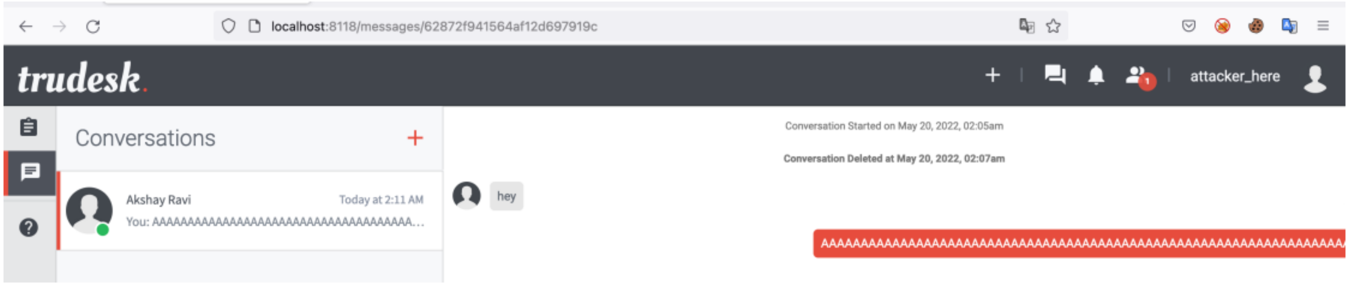
✓ Valid Reported on May 20th 2022

Steps to reproduce:

As an admin, start a new conversation with any member(normal user)
If the member(normal user) reply with a text of huge characters, (more than crores, etc)the admin may not able to access the dash board and its get started lagging, because the server get DOS

POC Screenshot:

[



localhost:8118/messages/62872f941564af12d697919c

Akshay Ravi Today at 2:11 AM
You: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...

Conversation Started on May 20, 2022, 02:05am

Conversation Deleted at May 20, 2022, 02:07am

hey

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

POC Video:

`https://www.mediafire.com/file/tzfqws14imvdfxr/trudesk_dos.mov/file`

Patch recommendation:

Limit the characters to max (5000 or 10000)

Impact

Denial of service

CVE
CVE-2022-1926

CVE-2022-1926
(Published)

Vulnerability Type

CWE-190: Integer Overflow or Wraparound

Severity
High (7.6)

Registry
Other

Affected Version
<=1.2.2

Visibility
Public

Status
Fixed

Found by

Akshay Ravi
@akshayravic09yc47
pro

Fixed by

Chris Brame
@polonel
unranked

This report was seen 498 times.

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

We have contacted a member of the **polonel/trudesk** team and are waiting to hear back
6 months ago

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

Chat with us

A **polonel/trudesk** maintainer has acknowledged this report 6 months ago

Chris Brame 6 months ago

Maintainer

This has been fixed and will release with version 1.2.3
I will update this report once released.

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 ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chris Brame marked this as fixed in **1.2.3** with commit **b7c151** 6 months ago

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation