huntr

UI REDRESSING in polonel/trudesk

0

✓ Valid Reported on May 18th 2022

Description

The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.

Proof of Concept

```
Go to this URL: https://clickjacker.io/test?url=https:%2F%2Fdocker.trudesk.io%2F
Observe that the website is getting embeded in an Iframe.
Observe that the headers x-frame-options and content-security-policy frame ancestors are missing.
```

Impact

Users are tricked into performing all sorts of unintended actions are such as typing in the password, clicking on ‘Delete my account’ button, liking a post, deleting a post, commenting on a blog. In other words all the actions that a normal user can do on a legitimate website can be done using clickjacking.

COUNTERMEASURES:

X-FRAME-OPTIONS is a security header to prevent clickjacking

References

- https://cwe.mitre.org/data/definitions/1021.html

CVE
CVE-2022-1803
(Published)

Vulnerability Type
CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Severity

High (8.4)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Vishal Vishwakarma
@vishalvishw10
pro

Fixed by

Chris Brame
@polonel
unranked

This report was seen 524 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 6 months ago Maintainer

This is fixed in v1.2.2. I will update this report once it is deployed.

Chat with us

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 **6ea9db** 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