

UI REDRESSING in ikus060/rdiffweb

0

✓ Valid

Reported on Sep 7th 2022

Description

Clickjacking is a portmanteau of two words 'click' and 'hijacking'. It refers to hijacking user's click for malicious intent. In it, an attacker embeds the vulnerable site in an transparent iframe in attacker's own website and overlays it with objects such as button using CSS skills. This tricks users to perform unintended actions on vulnerable website, thinking they are doing those on attacker's website. Clickjacking, also known as a "UI redress attack".

Proof of Concept

1. Go to this URL: <https://clickjacker.io/test?url=https:%2F%2Frdiffweb-den>
2. Observe that the website is getting embedded in an Iframe.
3. Observe that the headers x-frame-options and content-security-policy fra



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.

References

- <https://cwe.mitre.org/data/definitions/1021.html>
- <https://huntr.dev/bounties/47cc6621-2474-40f9-ab68-3cf62389a124/>
- <https://huntr.dev/bounties/a9ec1eef-98a0-4201-85ea-b111b3e86246/>

Chat with us

CVE-2022-3167

(Published)

Vulnerability Type

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

Severity

Critical (10)

Registry

Npm

Affected Version

<==1.2.15

Visibility

Public

Status

Fixed

Found by

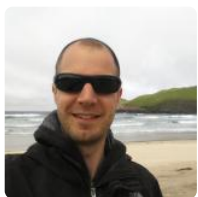


tharunavula

@tharunavula

amateur ✓

Fixed by



Patrik Dufresne

@ikus060

unranked ▾

This report was seen 596 times.

We are processing your report and will contact the **ikus060/rdiffweb** team within 24 hours.
3 months ago

Patrik Dufresne validated this vulnerability 3 months ago

Confirm as valid.

tharunavula has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

tharunavula [3 months ago](#)

Researcher

@admin kindly assign cve

Jamie Slome [3 months ago](#)

Admin

Happy to assign and publish a CVE once we get the go-ahead from the maintainer 👍

@Patrik - are you happy for us to assign and publish a CVE for this report for you?

Patrik Dufresne [3 months ago](#)

Maintainer

@Jamie Slome
Sure.

I'm already in process of getting this fixed.

Patrik Dufresne marked this as fixed in 2.4.1 with commit 7294bb [3 months ago](#)

Patrik Dufresne 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