

Hyperlink injection leads to redirect victim to malicious website in ikus060/rdiffweb

2



Valid

Reported on Sep 29th 2022

Description

Hyperlink Injection it's when attacker injecting a malicious link when sending an email invitation

Proof of Concept

- 1) Go to `https://rdiffweb-dev.ikus-soft.com/prefs/general`
- 2) Set your full name as "Your account has been hacked please visit evil.cc"
- 3) Save changes
- 4) Perform any activity that will lead to triggering an email on the victim
- 5) Victim will receive an email where `evil.com` is in the form of a hyperlink
- 6) As soon as he will click on `evil.com` he will be redirected to the malicious website

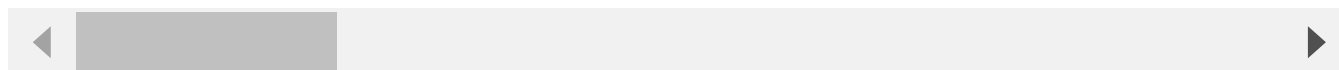
Let us consider a scenario where the user has left his account open in a browser

Mitigation: Full name is a field that requires only alphabets (in worst case scenario)

As soon as he click

Impact

An attacker can redirect victim to malicious website



References

- [Hackerone Report](#)

Chat with us

- [Hackerone Report](#)

CVE

CVE-2022-3438

(Published)

Vulnerability Type

CWE-601: Open Redirect

Severity

Medium (5.7)

Registry

Pypi

Affected Version

2.5.0a3

Visibility

Public

Status

Fixed

Found by



nehalr777

@nehalr777

master ▼

Fixed by



Patrik Dufresne

@ikus060

unranked ▼

This report was seen 761 times.

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

2 months ago

Patrik Dufresne validated this vulnerability 2 months ago

Chat with us

nehalr777 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Patrik Dufresne [2 months ago](#)

Maintainer

@admin Would it be possible to assign a CVE

Thanks

nehalr777 [2 months ago](#)

Researcher

@admin could we assign a CVE to this issue as requested by the @maintainer?

We have sent a fix follow up to the **ikus060/rdiffweb** team. We will try again in 7 days.
2 months ago

Patrik Dufresne marked this as fixed in **2.5.0a4** with commit **4d464b** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

nehalr777 [2 months ago](#)

Researcher

@admin can we assign a CVE for this? A fix has been deployed.

nehalr777 [2 months ago](#)

Researcher

@admin any updates on this?

Pavlos [a month ago](#)

Admin

The CVE has been published

Chat with us

Sign in to join this conversation

2022 © 4l8sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 4l8sec

[company](#)

[about](#)

[team](#)

Chat with us