

# Virtual defacement allows attacker to display any message of his choice in ikus060/rdiffweb

1



Valid

Reported on Sep 22nd 2022

## Description

This attack involves injecting malicious data into a page of a web application to feed misleading information to users of the application. This kind of attack is known as virtual defacement because the actual content hosted on the target's web server is not modified. The defacement is generated solely because of how the application processes and renders user-supplied input.

## Proof of Concept

Go to <https://rdiffweb-demo.ikus-soft.com>

Login using the credentials - admin , admin123

Visit url : <https://rdiffweb-demo.ikus-soft.com/>This website has been hacked and the confidential data of all users have been compromised and leaked to public . You can craft your personal message here .

Your message "This website has been hacked and the confidential data of all users have been compromised and leaked to public" will be displayed

Attack Scenario: Attacker constructs a malicious message.Attackers start posting this URL everywhere on social media. The message might get the attention of the media and several people might believe the news to be true which will cause huge business reputation and monetary damage

## Impact

A professionally crafted defacement, delivered to the right recipients in a convincing manner, could be picked up by the news media and have real-world effects on people's behavior, stock prices, and so on, to the attacker's financial benefit.

## Occurrences

Chat with us



124 1220

## References

- [Hackerone Report](#)

### CVE

CVE-2022-3301

(Published)

### Vulnerability Type

CWE-460: Improper Cleanup on Thrown Exception

### Severity

Medium (4.3)

### Registry

Other

### Affected Version

2.4.6

### Visibility

Public

### Status

Fixed

### Found by



nehalr777

@nehalr777

master ▼

### Fixed by



Patrik Dufresne

@ikus060

unranked ▼

This report was seen 835 times.

Chat with us

We are processing your report and will contact the **IKUS060/rdiffweb** team within 24 hours.  
2 months ago

**Patrik Dufresne** modified the Severity from High (7.3) to Medium (4.3) 2 months ago

**Patrik Dufresne** 2 months ago

Maintainer

@nehalr777 Plz update the affected version. and registry.

So basically, displaying the Path not found is a vulnerability !?

If so, let change the severity to something more accurate...

**nehalr777** 2 months ago

Researcher

Hello sir , thank you for looking into this. It affects the latest version of rdiffweb. The application is throwing back the requested endpoint in the form of a message, which in turn is the root cause of this. Just display a 404 and scrape out the error of the endpoint not found.

**nehalr777** 2 months ago

Researcher

The affected version is 2.4.6

**Patrik Dufresne** 2 months ago

Maintainer

Plz edit the "Affected Version" in the report. It currently define as 4.6 and should be 2.4.6. Once done, I will validate the report.

Thanks

**nehalr777** modified the report 2 months ago

**nehalr777** 2 months ago

Researcher

The affected version in the report has been updated.

The researcher has received a minor penalty to their credibility for miscalculating the severity.

**Patrik Dufresne** validated this vulnerability 2 months ago

Chat with us

Thanks

nehalr777 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

nehalr777 2 months ago

Researcher

Hello sir ,  
Are you happy to proceed with a CVE for this issue as well ?

Patrik Dufresne 2 months ago

Maintainer

Yes, let assign a CVE. @admin

nehalr777 2 months ago

Researcher

Hi @admin , I hope you are doing well . The maintainer has agreed to proceed with a CVE for this issue. Could you please assign a CVE?

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 2.4.8 with commit 5ac38b 2 months ago

Patrik Dufresne has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

test.py#L24-L220 has been validated ✓

Ben Harvie 2 months ago

Admin

A CVE has now been assigned to this report as requested :)

Chat with us



Sign in to join this conversation

2022 © 418sec

## huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

## part of 418sec

[company](#)

[about](#)

[team](#)

Chat with us