

## Secure token is missed when ivalid URL is entered in ikus060/rdiffweb

0



Valid

Reported on Sep 20th 2022

### Description

The cookie session\_id does not have secure attribute when the URL is invalid

### Proof of Concept

1.Login into the application. 2.Send the request <https://rdiffweb-demo.ikus-soft.com/browse/admin/MyWindowsLaptop/D/TC3080/test> .

### Impact

Secure attribute is necessary so the cookie is secure.

CVE

CVE-2022-3250

(Published)

Vulnerability Type

CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Severity

Medium (4.9)

Registry

Npm

Affected Version

2.5

Visibility

Public

Status

Fixed

Chat with us

Found by



irfansayyed-github

@irfansayyed-github

master ▼

Fixed by



Patrik Dufresne

@ikus060

unranked ▼

This report was seen 752 times.

We are processing your report and will contact the [ikus060/rdiffweb](#) team within 24 hours.

2 months ago

[Patrik Dufresne](#) 2 months ago

Maintainer

@irfansayyed-github Could you re-validate. Version 2.5.0 is not out yet. It's still in Beta.

Since version 2.4.2 (September 12), the secure attribute is added to the cookie when using https.

[irfansayyed-github](#) 2 months ago

Researcher

Yeah did.

<https://raw.githubusercontent.com/irfansayyed-github/irfansayyed-github/main/sde.png> you can verify that the cookie does not have secure attribute.

[Patrik Dufresne](#) 2 months ago

Maintainer

I see, that happen on error page.

[Patrik Dufresne](#) validated this vulnerability 2 months ago

[irfansayyed-github](#) has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

irfansayyed-github 2 months ago

Researcher

@admin could we get CVE?

Jamie Slome 2 months ago

Admin

Sure, once we get the go-ahead from the maintainer, we can assign and publish a CVE for you :)

Patrik Dufresne 2 months ago

Maintainer

@admin You may proceed with creation of a CVE. Thanks

Jamie Slome 2 months ago

Admin

Sorted :)

Patrik Dufresne marked this as fixed in 2.4.6 with commit `ac334d` 2 months ago

Patrik Dufresne has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

Chat with us

huntr

part of 418sec

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[company](#)

[about](#)

[team](#)

[Chat with us](#)