

Session_id without Secure attribute in ikus060/rdiffweb

1



Valid

Reported on Sep 9th 2022

Description

User's session id with secure attribute is false. This vulnerability makes user's cookies can be sent to the server with an unencrypted request over the HTTP protocol.

Proof of Concept

Open the browser and access to the website, in this scenario I use the demo website. Check the cookie in browser's dev tool and realize that the cookie with Secure attribute is false.

Impact

This vulnerability makes user's cookies can be sent to the server with an unencrypted request over the HTTP protocol.

CVE

CVE-2022-3174

(Published)

Vulnerability Type

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

Severity

High (7.5)

Registry

Other

Affected Version

>=2.4.1

Visibility

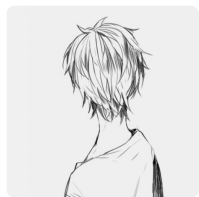
Public

Status

Fixed

Chat with us

Found by



Chuu

@uonghoangminhchau

amateur ✓

Fixed by



Patrik Dufresne

@ikus060

unranked ▼

This report was seen 765 times.

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

3 months ago

Chuu modified the report 3 months ago

Patrik Dufresne validated this vulnerability 3 months ago

Chuu has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chuu 3 months ago

Researcher

thank you.

Patrik Dufresne 2 months ago

Maintainer

@uonghoangminhchau

Could you or anyone else create a CVE report ?

Chuu 2 months ago

Chat with us

Researcher

@admin

Please help me to create CVE report.

Jamie Slome 2 months ago

Admin

All sorted 🙌 Once this report is marked as fixed (i.e. resolved), a CVE will automatically publish for this report with the CVE ID ([CVE-2022-3174](#)).

Patrik Dufresne 2 months ago

Maintainer

@chuu the affected version should be >=2.4.1

Jamie Slome 2 months ago

Admin

Sorted the affected version :)

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 [2.4.2](#) with commit [f2de23](#) 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

huntr

part of 418sec

Chat with us

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[company](#)

[about](#)

[team](#)

[Chat with us](#)