## huntr

## Session\_id without Secure attribute in ikus060/minarca



Reported on Sep 13th 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 get access to the minarca website, for this scenario I have used the demo/test 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.

### References

Mitre reference

CVE

CVE-2022-3251 (Published)

Vulnerability Type

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

Severity

High (7.5)

Registry

Other

Chat with us

### Visibility

Public

#### Status

Fixed

#### Found by



Fixed by



Patrik Dufresne
@ikus060

unranked V

This report was seen 829 times.

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

2 months ago

Patrik Dufresne validated this vulnerability 2 months ago

This vulnerability is valid. Was reported on Rdiffweb project.

Minarca will get fixed, whenever I upgrade Rdiffweb version embedded in Minarca.

Vanilla 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

Affected version should be 4.2.0

Chat with us

Researcher

Thank you. Yes, If I could edit the affected version It is 4.2.0 for the Minarca.

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

Vanilla 2 months ago Researcher

Hi @admin,

can you help me with the CVE ID for this report?

Jamie Slome 2 months ago Admin

Sorted the affected version:)

@Patrik - would you like me to assign a CVE for this report?

Patrik Dufresne 2 months ago Maintainer

@admin You may create a CVE for this report. Thanks

Jamie Slome 2 months ago Admin

Sorted:)

Vanilla 2 months ago Researcher

Thank you.!! @patrik @jamie

Patrik Dufresne marked this as fixed in 4.2.2 with commit 7b5c7e 2 months ago

Patrik Dufresne has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE x

Chat with us

#### 2022 © 418sec

#### huntr

home

hacktivity

leaderboard

FAO

contact us

terms

privacy policy

### part of 418sec

company

about

team