Improper Cache control allows attacker to view sensitive data in ikus060/rdiffweb

2

Valid Reported on Sep 22nd 2022

Description

Due to improper cache control an attacker can view sensitive information even if he is not logged into the account

Proof of Concept

Go to https://rdiffweb-demo.ikus-soft.com/login/ and login into your account using given credentials
Go to https://rdiffweb-demo.ikus-soft.com/admin/logs and this endpoint has the entire log
Click on Logout
Now press the back button of your browser
You will notice that you are still able to view the sensitive data/log files
Mitigation: Cache-Control: private, no-cache, no-store, max-age=0 Pragma: no-cache Expires: 0

Impact

An attacker can get access to sensitive information due to improper cache control

Occurrences

admin_logs.html L1-L34

References

- https://cwe.mitre.org/data/definitions/525.html

CVE

CVE-2022-3292
(Published)

Vulnerability Type

CWE-524: Use of Cache Containing Sensitive Information

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 857 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

If I understand it well, admin_logs is not the only page affected. Almost any page contain sensitive information. e.g.: The browser page contain list of personal file and di
the user. etc.

So I should probably apply these headers to all the pages except the static file like css, javascript,

etc.

nehalr777 2 months ago Researcher

Yes sir , you are right all the sensitive endpoints are vulnerable to this issue.
Applying this header to all sensitive endpoints would fix this issue :)

We have contacted a member of the **ikus060/rdiffweb** team and are waiting to hear back
2 months ago

Patrik Dufresne assigned a CVE to this report 2 months ago

Patrik Dufresne validated this vulnerability 2 months ago

nehalr777 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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 **240678** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

admin_logs.html#L1-L34 has been validated ✔

Sign in to join this conversation