Error page is default and leak error information in ikus060/rdiffweb

0

Valid Reported on Sep 9th 2022

Description

Information is leak in error page and this can support for other vulnerabilities.

Proof of Concept

Whenever trying to input anything meaningless after the link https://rdiffweb-demo.ikus-soft.com/ the error page will appear. Example: https://rdiffweb-demo.ikus-soft.com/* https://rdiffweb-demo.ikus-soft.com/' https://rdiffweb-demo.ikus-soft.com/admin/

Impact

Leaking information. Chance for other vulnerabilities.

CVE
CVE-2022-3175
(Published)

Vulnerability Type
CWE-756: Missing Custom Error Page

Severity
Medium (5.3)

Registry
Other

Affected Version
>=2.4.1

Visibility
Public

Status

Fixed

Found by

Chuu

@uonghoangminhchau

amateur

Fixed by

Patrik Dufresne

@ikus060

unranked

This report was seen 697 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 3 months ago Maintainer

The demo server is running with "debug" intentionally enabled.
By default, rdiffweb is running without "debug" enabled. So I would not consider this a vulnerabilities.

Patrik Dufresne 3 months ago Maintainer

Nevermind. Debug mode is disable and error_page still leak a stacktrace

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

@chuu
Would you create a CVE for this ?

Chuu 2 months ago Researcher

@admin
Please help me to create a 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-2022-3175`).

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 **233bef** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Chuu 2 months ago

@Patrik

Thank you.
By the way, I have a question, does this have bounty ?

Jamie Slome 2 months ago **Admin**

We are currently not rewarding bounties on these types of reports. To see the projects you can get bounties for, see our list here.

> Sign in to join this conversation