Path Traversal (CWE-22) leak sensitive data in ikus060/rdiffweb

0

Valid Reported on Oct 1st 2022

Description

Path Traversal successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of the restricted directory on the remote server.

Proof of Concept

 poc!!
Note: If you can not see the poc image , you can follow this link https://imgur.com/a/1svTNB4

Impact

Arbitrary file read. This could leak sensitive system files or any file present on the system.

CVE
CVE-2022-3389
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
High (8.2)

Registry
Other

Affected Version
lastest

Visibility
Public

Status

Fixed

Found by

Hoang Van Hiep

@sk4rl1ght

legend

Fixed by

Patrik Dufresne

@ikus060

unranked

This report was seen 1,139 times.

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

Hoang Van Hiep 2 months ago Researcher

this is my first report on huntr.dev, so i don't know how to push image correctly :D

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

Hoang Van Hiep 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

@t1g3r0x I'm working on a fix. ASAP.

Another question for you. What led you to test Rdiffweb?

Another question for you: What led you to test Rdiffweb?

Hoang Van Hiep 2 months ago Researcher

you know, testing the open source like Rdiffweb or another one, is also a way to improve penetration testing skills :D

Patrik Dufresne marked this as fixed in 2.4.10 with commit 323383 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Hoang Van Hiep 2 months ago Researcher

when is cve public?

Hoang Van Hiep 2 months ago Researcher

@admin

Pavlos a month ago Admin

It's public now :) It takes 24hrs usually

Sign in to join this conversation