

# No Limit in length of root directory name , results in memory consumption/DOS attack in ikus060/rdiffweb



Valid

Reported on Sep 24th 2022

## Description

There must be a fixed length for user input parameters like root directory name. Allowing users to enter long strings may result in a DOS attack or memory corruption

## Proof of Concept

1)Go to <https://rdiffweb-demo.ikus-soft.com/admin/users> endpoint . 2)Click on add user  
3)Here you will see that there is no limit for the root directory name length that allows a user to to set a very long string as long as 1 million characters 4)This may possible result in a memory corruption/DOS attack

Mitigation: There must be a fixed length for the root directory name - upto 256 characters

## Impact

Allows an attacker to set a root directory name with long string leading to memory corruption/possible DOS attack

## Occurrences



admin\_users.html L1-L122

CVE

CVE-2022-3295

(Published)

Vulnerability Type

CWE-770: Allocation of Resources Without Limits or Throttling

Severity

Medium (5.3)

Chat with us

Registry  
Pypi

Affected Version  
2.4.6

Visibility  
Public

Status  
Fixed

Found by



nehalr777

@nehalr777

master ▼

Fixed by



Patrik Dufresne

@ikus060

unranked ▼

This report was seen 702 times.

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

**Patrik Dufresne** marked this as fixed in **2.4.8** with commit **667657** 2 months ago

**Patrik Dufresne** has been awarded the fix bounty ✓

Chat with us

Patrik Dufresne has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

admin\_users.html#L1-L122 has been validated ✓

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us