

# No Limit in "title" length while adding SSH key , results in memory consumption/DOS attack in ikus060/rdiffweb

2



Valid

Reported on Sep 24th 2022

## Description

There must be a fixed length for user input parameters like "title" while adding SSH key. 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/prefs/sshkeys#> endpoint . 2)Click on add SSH key. 3)Here you will see that there is no limit for the "title" while adding SSH key that allows a user to to set a very long string as long as 1 million characters . 4)This may possibly result in a memory corruption/DOS attack.

Mitigation: There must be a fixed length for the "title" while adding SSH key - upto 256 characters

## Impact

Allows an attacker to set a "title" with long string leading to memory corruption/possible DOS attack

## Occurrences



prefs\_sshkeys.html L1-L55

CVE

CVE-2022-3298

(Published)

Vulnerability Type

CWE-770: Allocation of Resources Without Limits or Throttling

Severity

Chat with us

Severity

Medium (5.3)

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 791 times.

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

2 months ago

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

Chat with us

Patrik Dufresne marked this as fixed in 2.4.8 with commit 626cca 2 months ago

Patrik Dufresne has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

prefs\_sshkeys.html#L1-L55 has been validated ✓

nehalr777 2 months ago

Researcher

@admin this issue has been fixed. The maintainer has already assigned a CVE for this issue. Could we please publish the CVE?

Ben Harvie 2 months ago

Admin

Hi nehalr777,

The publishing of a CVE will happen automatically within 24 hours of the fix being submitted, so it should be published shortly. Happy hunting!

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

part of 418sec

company

about

team

Chat with us

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)