huntr

No limit in length of "Token name" parameter results in DOS attack /memory corruption in ikus060/rdiffweb

3



✓ Valid Reported on Sep 29th 2022

Proof of Concept

- 1)Go to https://rdiffweb-dev.ikus-soft.com/prefs/tokens endpoint .
- 2)You will see a field called "Token name"
- 3)Here you will see that there is no limit for the "Token name" parameter t
- 4) This may possibly result in a memory corruption/DOS attack.

Mitigation: There must be a fixed length for the "Token name" parameter upt

Impact

Allows an attacker to set a "Token name" with long string leading to memory



CVE

Vulnerability Type

CWE-770: Allocation of Resources Without Limits or Throttling

Severity

Registry

Affected Version

Chat with us

Visibility Public

Status Fixed

Found by



nehalr777
@nehalr777
master •

Fixed by



Patrik Dufresne
@ikus060
unranked v

This report was seen 797 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 2.5.0a3 with commit b62c47 2 months ago

Patrik Dufresne has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE x

Chat with us

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team