No limit in email length may result in a possible DOS attack in ikus060/rdiffweb

1

Valid Reported on Sep 22nd 2022

Description

As per RFC the maximum length allowed for an email address is 255 characters. However, rdiffweb don't validate email length, so you can add email addresses that exceed 255 characters. Through this, if you sign up for an email with a length of 1 million or more and log in, withdraw, or change your email, the server may cause DOS due to overload.

Proof of Concept

Go to https://rdiffweb-demo.ikus-soft.com/prefs/general
You can now change the email associated with your account from this endpoint
Set a very long email that exceeds 1000 characters
You will see that the long email is readily accepted and there is no fixed length for this user input parameter
Mitigation: The email parameter must have a specific user input length

Impact

An attacker can store a large email address as per his requirement which will possibly lead to a DOS attack / Buffer Overflow

Occurrences

config.py L112-L164

References

- Hackerone Report

CVE
CVE-2022-3272
(Published)

Vulnerability Type
CWE-130: Improper Handling of Length Parameter Inconsistency

Severity
Medium (5.3)

Registry
Other

Affected Version
2.4.6

Visibility
Public

Status
Fixed

Found by

nehalr777
@nehalr777
master

Fixed by

Patrik Dufresne
@ikus060
unranked

This report was seen 748 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

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 **2.4.8** with commit **667657** 2 months ago

Patrik Dufresne has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

config.py#L112-L164 has been validated ✔

Sign in to join this conversation