huntr

Business Logic error lead to race condition in erudika/para
0

✔ **Valid** Reported on May 18th 2022

Description

I have found Business logic Bug in para application free User can create more than 1 app even after App limit reached

Proof of Concept

1 - Go to https://paraio.com/apps

2 - Create a new app

3- Enter the name of app

4- Intercept the request in burp suite and send into intruder and select payload as number and select number

5- Start Attack

Video Poc -: https://drive.google.com/file/d/1xyUY-QK0y_XIPKjfkh-nib6HsTVELP9R/view?usp=sharing

Screenshot of POC :- https://drive.google.com/file/d/1Mqr9WNqWWwcPBN8xqxITYwvV8wXhoLbx/view?usp=sharing

Impact

Business Impact
Free User can create more than 1 so he don't have to pay money for this services so this is very dangerous for your business

References

- https://cwe.mitre.org/data/definitions/366.html

Chat with us

CVE
CVE-2022-1848
(Published)

Vulnerability Type
CWE-840: Business Logic Errors

Severity
Critical (9)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Vishal Vishwakarma
@vishalvishw10
pro ⌄

Fixed by

Alex Bogdanovski
@albogdano
maintainer

We are processing your report and will contact the **erudika/para** team within 24 hours.
6 months ago

We have contacted a member of the **erudika/para** team and are waiting to hear back
6 months ago

We have sent a follow up to the **erudika/para** team. We will try again in 7 d⸍

Chat with us

Alex Bogdanovski validated this vulnerability 6 months ago

Alex Bogdanovski validated this vulnerability 6 months ago

Vishal Vishwakarma has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Alex Bogdanovski marked this as fixed in **1.45.11** with commit **fa677c** 6 months ago

Alex Bogdanovski has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

Vishal 6 months ago   Researcher

@admin can you please assigned as cve

Jamie Slome 6 months ago   Admin

Sorted 👍 Anything else I can support with?

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

part of 418sec

company

about

team

Chat with us

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us