# Inefficient Regular Expression Complexity in nervjs/taro





# Description

A ReDoS (regular expression denial of service) flaw was found in the <code>@tarojs/helper</code> package. An attacker that is able to provide crafted input as url may cause an application to consume an excessive amount of CPU.

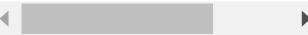


# Proof of Concept

Create the following poc.mjs

### // PoC.mjs

```
import pkg from '@tarojs/helper';
const {REG_URL} = pkg;
var time = Date.now();
var time_cost = Date.now() - time;
console.log("Time taken to validate : " + time_cost+" ms")
```



Execute the following command in another terminal:

```
npm i @tarojs/helper
node poc.js
```

### Check the Output:

Time taken to validate : 44880 ms



## Impact

This vulnerability is capable of exhausting system resources and leads to crashes. Ideally, validation should be done within 1-10 milliseconds, but in the above case, it's 44 seconds.

# Occurrences

TS constants.ts L107

### Vulnerability Type

### Severity

Affected Version

### Status

#### Found by



ready-research



ready-research

We created a <b>GitHub Issue</b> asking the maintainers to create a <b>SECURITY.md</b> a year ago
ready-research submitted a patch a year ago
ready-research a year ago Researcher
After applying the patch output is Time taken to validate: 4 ms
ready-research a year ago Researcher
@admin It seems maintainers recommending submitting an issue using https://issue.taro.zone/If we open an issue directly in GitHub, the bot will automatically closing that issue. Can you please look into this?
Z-Old a year ago Admin
Hey ready-research, thanks for making us aware of this.
Strange form as there is no field for leaving an email.
Here's my suggestion. Fill out the form and ask them to email security@huntr.dev and CC yourself in the final text field. This way, should they respond, we can both stay in the loop.
Does that sound reasonable to you?
chenjiajian validated this vulnerability a year ago
ready-research has been awarded the disclosure bounty 🗸
The fix bounty is now up for grabs
chenjiajian marked this as fixed with commit acadb6 a year ago
ready-research has been awarded the fix bounty ✓
This vulnerability will not receive a CVE 🗴
constants.ts#L107 has been validated ✓
Jamie Slome a year ago Admin
CVE published! 🞉
Sign in to join this conversation

# huntr part of 418sec

hacktivity
leaderboard

eaderboard FAQ

rms

company about team