New issue

Jump to bottom

Fix ReDoS when parsing colors #3382

Merged

piaskowyk merged 1 commit into `software-mansion:main` from `matias-la:fix-redos-upstream` on Jul 25

matias-la commented on Jul 12 Contributor

Description

The regular expression used to parse numbers could be abused to cause a denial of service if the color to be parsed is controlled by an attacker.

For information about this vulnerability, see https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS.

Changes

Changed the code so the new regex isn't vulnerable, since there's always only one possible path to take given any input.

Here is a proof-of-concept of how I made the existing regular expression cause a 100% CPU usage for several seconds, after being interrupted:

```
Welcome to Node.js v14.19.3.
Type ".help" for more information.
> (new RegExp('^[-+]?\\d*\\.?\\d+$')).test(`${'1'.repeat(1e6)}z`)
^CUncaught Error: Script execution was interrupted by `SIGINT`
    at Script.runInThisContext (vm.js:134:12)
    at REPLServer.defaultEval (repl.js:566:29)
    at bound (domain.js:421:15)
    at REPLServer.runBound [as eval] (domain.js:432:12)
    at REPLServer.onLine (repl.js:909:10)
    at REPLServer.emit (events.js:412:35)
    at REPLServer.emit (domain.js:475:12)
    at REPLServer.Interface._onLine (readline.js:434:10)
    at REPLServer.Interface._line (readline.js:791:8)
```

```
    at REPLServer.Interface._ttyWrite (readline.js:1136:14) {
  code: 'ERR_SCRIPT_EXECUTION_INTERRUPTED'
}
> (new RegExp('^[-+]?\\d*(?:\\.\\d*)?$')).test(`${'1'.repeat(1e6)}z`) // the new regex works fine
false
>
```

Checklist

- [x] Included code example that can be used to test this change
- [ ] Updated TS types
- [ ] Added TS types tests
- [ ] Added unit / integration tests
- [ ] Updated documentation
- [ ] Ensured that CI passes

👍 1

 Fix ReDoS when parsing colors ✓ 7adf06d

 **piaskowyk** self-requested a review 4 months ago

 **piaskowyk** self-assigned this on Jul 25

piaskowyk approved these changes on Jul 25

View changes

 **piaskowyk** left a comment Member

Hey **@matias-la**, Thanks for your PR!

 **piaskowyk** merged commit **6025581** into `software-mansion:main` on Jul 25

1 check passed

View details

 piaskowyk pushed a commit that referenced this pull request on Jul 25

 Fix ReDoS when parsing colors (#3382) ··· 4921679

petrusek commented on Jul 26 • edited ▾ Contributor

@matias-la @piaskowyk ... just to be sure, is it OK that the new regex accepts empty string and returns true?

OLD

```
> (new RegExp('^[-+]?\\d*\\.?\\d+$')).test('')
false
```

NEW

```
> (new RegExp('^[-+]?\\d*(?:\\.\\d*)?$')).test(``)
true
```

👍 1

piaskowyk mentioned this pull request on Jul 28

Prevent empty string match in color regex #3419

Merged

matias-la commented on Aug 1 Contributor Author

Oops, nice catch! I hadn't notice that. The change in #3419 look good, as it prevents empty strings from matching while also not being vulnerable to ReDoS.

👍 1

piaskowyk added a commit that referenced this pull request on Aug 2

`Prevent empty string match in color regex (#3419) ...` ✕ `6bdaf24`

piaskowyk added a commit that referenced this pull request on Aug 2

`Prevent empty string match in color regex (#3419) ...` `8a92790`

EvertEt added a commit to EvertEt/normalize-css-color that referenced this pull request on Oct 27

`Fix ReDoS when parsing colors ...` `78fce4d`

 **EvertEt** mentioned this pull request on Oct 27

Fix ReDoS when parsing colors rnc-archive/normalize-css-color#1

Open

5 tasks

Reviewers

 **piaskowyk** ✓

Assignees

 **piaskowyk**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants