New issue

Jump to bottom

Regular Expression Denial of Service (ReDoS) in dat.gui #278

Closed yetingli opened this issue on Oct 6, 2020 · 0 comments

yetingli commented on Oct 6, 2020 Contributor

Type of Issue
Potential Regex Denial of Service (ReDoS)

Description
The vulnerable regular expression is located in

dat.gui/src/dat/color/interpret.js
Line 61 in 51d1a37

```
61      const test = original.match(/^rgb\(\s*(.+)\s*,\s*(.+)\s*,\s*(.+)\s*\)/);
```

dat.gui/src/dat/color/interpret.js
Line 79 in 51d1a37

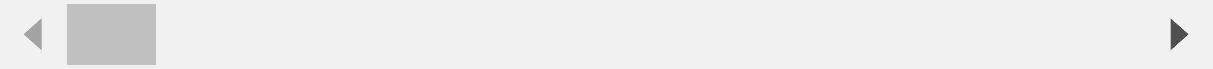
```
79      const test = original.match(/^rgba\(\s*(.+)\s*,\s*(.+)\s*,\s*(.+)\s*,\s*(.+)\s*\)/);
```

The ReDOS vulnerability of the regex is mainly due to the sub-pattern `\s*(.+)\s*` and can be exploited with the following string `"rgb("+" " * 5000`

You can execute the following code to reproduce ReDos

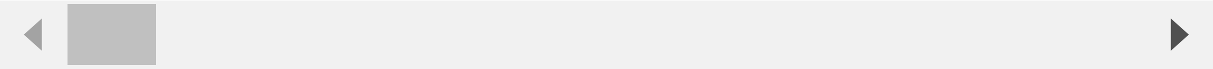
```
<script type="text/javascript" src="build/dat.gui.js"></script>
<script type="text/javascript">
var gui = new dat.gui.GUI();
var Options = function() {
        this.color0 = "rgb(
};

window.onload = function() {
        var options = new Options();
        gui.addColor(options, 'color0');
};
</script>
```



```
<script type="text/javascript" src="build/dat.gui.js"></script>
<script type="text/javascript">
var gui = new dat.gui.GUI();
var Options = function() {
        this.color0 = "rgba(
};

window.onload = function() {
        var options = new Options();
        gui.addColor(options, 'color0');
};
</script>
```



yetingli mentioned this issue on Oct 6, 2020

Fix ReDos in CSS_RGB and CSS_RGBA #279

Merged

yetingli closed this as completed on Nov 24, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

1 participant