New issue

Jump to bottom

CSS injection with width and height options #546

Closed **ankane** opened this issue on Aug 4, 2020 · 5 comments

ankane commented on Aug 4, 2020 • edited ▾ Owner

The Chartkick Ruby gem is vulnerable to CSS injection if user input is passed to the `width` or `height` option. This vulnerability has been assigned the CVE identifier CVE-2020-16254.

Versions Affected: 3.3.2 and below
Fixed Versions: 3.4.0

Impact

Chartkick is vulnerable to CSS injection if user input is passed to the `width` or `height` option.

```
<%= line_chart data, width: params[:width], height: params[:height] %>
```

An attacker can set additional CSS properties, like:

```
<%= line_chart data, width: "100%; background-image: url('http://example.com/image.png')" %>
```

All users running an affected release should upgrade.

Technical Details

Chartkick uses `ERB::Util.html_escape` to escape the width and height. This prevents XSS, but does not escape semicolons, which allows CSS additional properties to be set. Chartkick now limits width and height values to alphanumeric and % (this prevents some valid values like `calc()` but keeps things simple).

ankane closed this as completed on Aug 4, 2020

ankane mentioned this issue on Aug 4, 2020

Added CVE-2020-16254 for chartkick rubysec/ruby-advisory-db#453
Merged

cernyjakub commented on Oct 3, 2020

Hello! My app stopped working after updating to 3.4 - I use `rem` units to set height.

I think all units should be whitelisted - in other apps I also use `vw`, `wh` or `em` ...

regards!
jakub

ankane commented on Oct 3, 2020 Owner Author

Hey **@cernyjakub**, can you share the exact values you're trying to use that aren't working?

cernyjakub commented on Oct 4, 2020

This is the exact line from Sentry trace:

```
= bar_chart data, :height => "#{src.keys.size * 1.75}rem"
```

I use `rem` with float value - maybe the float is the glitch?

ankane added a commit that referenced this issue on Oct 5, 2020

`Relaxed validation for width and height options - #546` ✓ 1092181

ankane commented on Oct 6, 2020 Owner Author

Hey **@cernyjakub**, 3.4.1 was just released which allows for the `.` character.

cernyjakub commented on Oct 7, 2020

Thanks for patching this, works fine for me!

This was referenced on Mar 12, 2021

build(deps): bump chartkick from 3.3.1 to 3.4.2 freesteph/watchdog#13

Open

Bump chartkick from 3.3.2 to 3.4.0 arvmaster/PACE#2

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants