Regular Expression Denial of Service (REDoS)

Moderate liZe published GHSA-hq37-853p-g5cf on Jan 6, 2021

Package

cairosvg (pypi)

Affected versions	Patched versions
< 2.5.1	2.5.1

Description

Doyensec Vulnerability Advisory

- Regular Expression Denial of Service (REDoS) in cairosvg
- Affected Product: CairoSVG v2.0.0+
- Vendor: https://github.com/Kozea
- Severity: Medium
- Vulnerability Class: Denial of Service
- Author(s): Ben Caller (Doyensec)

Summary

When processing SVG files, the python package CairoSVG uses two regular expressions which are vulnerable to Regular Expression Denial of Service (REDoS).
If an attacker provides a malicious SVG, it can make cairosvg get stuck processing the file for a very long time.

Technical description

The vulnerable regular expressions are

CairoSVG/cairosvg/colors.py
Lines 190 to 191 in 9c4a982

```
190     RGBA = re.compile(r'rgba\([ \n\r\t]*(.+?)[ \n\r\t]*\)')
191     RGB = re.compile(r'rgb\([ \n\r\t]*(.+?)[ \n\r\t]*\)')
```

The section between 'rgb(' and the final ')' contains multiple overlapping groups.

Since all three infinitely repeating groups accept spaces, a long string of spaces causes catastrophic backtracking when it is not followed by a closing parenthesis.

The complexity is cubic, so doubling the length of the malicious string of spaces makes processing take 8 times as long.

Reproduction steps

Create a malicious SVG of the form:

```
<svg width="1" height="1"><rect fill="rgb(                    ;"/></svg>
```

with the following code:

```
'<svg width="1" height="1"><rect fill="rgb(' + (' ' * 3456) + ';"/></svg>'
```

Note that there is no closing parenthesis before the semi-colon.

Run cairosvg e.g.:

```
cairosvg cairo-redos.svg -o x.png
```

and notice that it hangs at 100% CPU. Increasing the number of spaces increases the processing time with cubic complexity.

Remediation

Fix the regexes to avoid overlapping parts. Perhaps remove the [\n\r\t]* groups from the regex, and use .strip() on the returned capture group.

Disclosure timeline

- 2020-12-30: Vulnerability disclosed via email to CourtBouillon

Severity

Moderate

CVE ID

CVE-2021-21236

Weaknesses

No CWEs

Credits

 b-c-ds