domenic / svg2png Public

Code Issues 30 Pull requests 6 Actions Projects Wiki ···

New issue

Jump to bottom

SSRF and Server Side XSS #117

Open **21k** opened this issue on Apr 16, 2020 · 3 comments

21k commented on Apr 16, 2020 • edited

this package uses phantomjs to render a xml snippet to image，thus the xml can be any html ,script.
As the render process runs at backend,so there are ssrf and server side xss risks.

21k commented on Apr 16, 2020 Author

```
var svg2png=require('svg2png')

svg2png(Buffer.from(`
<script> document.write(1111111111111); // some xhr for ssrf code </script>`)).then(buffer => fs.writeFileSync("dest.png", buffer))
```

huntr-helper commented on May 3, 2020

👋 Hey! We've recently opened a bug bounty against this issue, so if you want to get rewarded 💰 for fixing this vulnerability 🕷, head over to https://huntr.dev!

JamieSlome commented on May 8, 2020

Fix suggested here #119! 🍰

JamieSlome mentioned this issue on May 8, 2020

huntr.dev - Cross Site Scripting (XSS) Fix #119

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants