New issue

Jump to bottom

Security Fix for Command Injection - huntr.dev #10644

Merged **gaearon** merged 3 commits into `facebook:master` from `418sec:1-npm-react-dev-utils` on Mar 8, 2021

Conversation 20 Commits 3 Checks 17 Files changed 1

huntr-helper commented on Mar 3, 2021

@zpbrent (https://huntr.dev/users/zpbrent) has fixed a potential Command Injection vulnerability in your repository 🔨. For more information, visit our website (https://huntr.dev/) or click the bounty URL below...

Q | A
Version Affected | *
Bug Fix | YES
Original Pull Request | 418sec#2
Vulnerability README | https://github.com/418sec/huntr/blob/master/bounties/npm/react-dev-utils/1/README.md

User Comments:

📊 Metadata *

react-dev-utils includes some utilities used by Create React App.

The function getProcessForPort in react-dev-utils is vulnerable to command injection.

Bounty URL: **https://www.huntr.dev/bounties/1-npm-react-dev-utils/**

⚙️ Description *

Used child_process.execFileSync() instead of child_process.execSync().

💻 Technical Description *

The use of the child_process function execSync() is highly discouraged if you accept user input and don't sanitize/escape them. This PR replaces it with execFileSync() which mitigates any possible Command Injections as it accepts input as arrays.

🐛 Proof of Concept (PoC) *

Create a .js file with the content below and run it, then the file pzhou@shu can be illegally created.

// poc.js
var getProcessForPort = require('react-dev-utils/getProcessForPort');

getProcessForPort('11;$(touch pzhou@shu)');

🔥 Proof of Fix (PoF) *

use "return execFileSync('lsof', ['-i:'+port, '-P', '-t', '-sTCP:LISTEN'], execOptions)" to replace "return execSync('lsof -i:' + port + ' -P -t -sTCP:LISTEN', execOptions)"

👍 User Acceptance Testing (UAT)

var getProcessForPort = require('react-dev-utils/getProcessForPort');

getProcessForPort(3000) // works correctly

🔗 Relates to...

418sec/huntr#1962

zpbrent and others added 2 commits last year

`Update getProcessForPort.js` 7c9e253

`Merge pull request #2 from zpbrent/patch-3` ··· ✕ ab46fb8

huntr-helper requested review from **ianschmitz**, **iansu**, **mrmckeb** and **petetnt** as code owners last year

facebook-github-bot added the CLA Signed label on Mar 3, 2021

gaearon commented on Mar 3, 2021 Member

Who signed the CLA? I'm a bit confused. **@zpbrent** Did you sign it?

gaearon commented on Mar 3, 2021 Member

To be clear for random readers — this vulnerability does not affect Create React App itself, only people who are using its internal utilities directly.

JamieSlome commented on Mar 3, 2021

@gaearon - we have the CLA signed from our side for the `huntr-helper` account.

Perhaps the CLA is already signed by **@zpbrent** as well?

Cheers! 🍰

gaearon commented on Mar 3, 2021 Member

I think ideally we'd have **@zpbrent** sign the CLA explicitly since they're the primary author.

JamieSlome commented on Mar 3, 2021

@gaearon - sure, makes sense!

@zpbrent, are you able to sign the CLA:

https://code.facebook.com/cla

JamieSlome commented on Mar 3, 2021

On a side note, **@gaearon**, would it make sense for the bot to check for CLAs signatures against all PR commit users?

gaearon commented on Mar 3, 2021 Member

Yea I flagged this to our tooling team but it will involve some work and probably won't happen very soon.

JamieSlome commented on Mar 3, 2021

@gaearon 👍

zpbrent commented on Mar 3, 2021 Contributor

> **@gaearon** - sure, makes sense!
>
> **@zpbrent**, are you able to sign the CLA:
>
> https://code.facebook.com/cla

@gaearon and **@JamieSlome** thanks for your advice, and I have signed the CLA just now.

❤️ 1

zpbrent commented on Mar 3, 2021 Contributor

> Yea I flagged this to our tooling team but it will involve some work and probably won't happen very soon.

@gaearon would you kindly help me to request a CVE for this vul. (I am also the discloser of this vul.), many thanks!

JamieSlome commented on Mar 4, 2021

@zpbrent - great, thanks for the quick follow up! 👍

gaearon commented on Mar 4, 2021 Member

CVE-2021-24033

gaearon commented on Mar 4, 2021 Member

Have you verified that this function works on Windows?

zpbrent commented on Mar 4, 2021 Contributor

> CVE-2021-24033

Thanks for the CVE :-)

zpbrent commented on Mar 4, 2021 Contributor

> Have you verified that this function works on Windows?

Sorry, I have not verified it in the Windows.

`Update getProcessForPort.js` ✕ `9798616`

gaearon merged commit **f5e415f** into `facebook:master` on Mar 8, 2021

1 of 8 checks passed

View details

JamieSlome commented on Mar 8, 2021

@gaearon - thanks for the merge! 👍

If you are interested in more fixes like this in the future, you can let security researchers know that they can win bounties protecting your repository by copying this small code snippet into your README.md:

```
[![huntr](https://cdn.huntr.dev/huntr_security_badge_mono.svg)](https://huntr.dev)
```

security bounty | up to $750 + CVE

---

gaearon commented on Mar 8, 2021 — Member

This case is a bit awkward because this vulnerability is extremely unlikely in practice (CRA's usage of this function does not supply user input there, and I find it difficult to imagine a situation in which you would pass it in the context of this tool). So while I appreciate a fix, I expect that this will cause downstream maintenance burden because once the CVE goes out, we'll get dozens of people asking to backport this fix to old majors because audit tools scream at them, and people don't understand the nuance of when a vulnerability applies or not. I understand vulnerabilities need to be addressed but the noise/signal ratio has been pretty bad historically and I'm not sure I'd like to incentivise increasing it.

JamieSlome commented on Mar 9, 2021

@gaearon - appreciate your comments above...

I am curious about your comments about the noise/signal ratio that you have seen historically. I would be eager to get some more of your thoughts/feedback in this area.

Perhaps I could shoot over an e-mail with some questions or schedule a 15-minute call? ☎

---

gaearon commented on Mar 9, 2021 — Member

Sure, email sounds fine. My username at fb dot com.

Past context:

- ✓ react-dev-utils uses a vulnerable version of immer as a dependency #10411 (comment)
- ✓ OWASP Dependency Check found 83 Critical Security Vulnerabilities in react-scripts:4.0.1, 3.4.4 package #10323
- ✓ Report High severity vulnerability in react-scripts 3.4.3 dependencies #9842 (comment)
- ✓ Security Vulnerabilities detected in the depedency packages requires an update #9815 (comment)
- ✓ High severity vulnerability detected by audit in react-scripts 3.4.2 dependencies #9469 (comment)

JamieSlome commented on Mar 9, 2021

@gaearon - great! 👍

Just had a browse through those PRs/comments. Certainly come across other maintainers experiencing similar issues.

I will get some questions together and send them over to you on your FB e-mail.

Cheers! 🍰

👍 2

---

notjustinshaw mentioned this pull request on Mar 15, 2021

[Security] patch for react-dev-utils package BlubbrDev/site#28

✓ Closed

mstelz mentioned this pull request on Apr 6, 2021

Security Fix for Command Injection - huntr.dev (#10644) blackarctic/create-react-app#15

Closed

akxcv pushed a commit to akxcv/create-react-app that referenced this pull request on Apr 28, 2021

`Security Fix for Command Injection - huntr.dev (facebook#10644)` … d70d014

raix pushed a commit to raix/create-react-app that referenced this pull request on May 14, 2021

`Merge remote-tracking branch 'upstream/master'` … ✓ b6ef26d

raix pushed a commit to raix/create-react-app that referenced this pull request on May 14, 2021

`Merge remote-tracking branch 'upstream/wp5' into webpack5-update` … ✓ 0170343

wombleton pushed a commit to AurorNZ/create-react-app that referenced this pull request on May 31, 2021

`Security Fix for Command Injection - huntr.dev (facebook#10644)` … ebb750e

th13ntc mentioned this pull request on Jul 14

Security Fix for Command Injection #12590

Open

Reviewers

ianschmitz ●

iansu ●

mrmckeb ●

petetnt ●

Assignees

No one assigned

Labels

CLA Signed

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

5 participants