

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

Exponential ReDoS (CVE-2021-23424) #19

🔒 Closed b-c-ds opened this issue on May 7, 2021 · 22 comments · Fixed by [#20](#) or [gebhardttr/ansi-html#1](#)

b-c-ds commented on May 7, 2021 • edited

Posting here as unable to contact maintainer.

Doyensec Vulnerability Advisory

- Regular Expression Denial of Service (ReDoS) in ansi-html
- Affected Product: ansi-html <= 0.0.7
- Vendor: <https://github.com/Tjatse>
- Severity: Low
- Vulnerability Class: Denial of Service
- Status: Open
- Author(s): Ben Caller (Doyensec)

SUMMARY

The npm package ansi-html uses a regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS). If an attacker provides a malicious string, ansi-html will get stuck processing the input for an extremely long time.

TECHNICAL DESCRIPTION

The vulnerable regular expression is

```
\033\[ (\\d+)*m
```

[ansi-html/index.js](#)
Line 62 in 99ec49e

```
62      var ret = text.replace(/\033\[ (\\d+)*m/g, function (match, seq) {
```

Due to the `(\\d+)*` part, this regular expression has catastrophic backtracking when given a long string of digits.

The behaviour occurs as long as the digits are not followed immediately by an 'm'.

The complexity is exponential: increasing the length of the malicious string by one makes processing take about twice as long.

REPRODUCTION STEPS

In nodejs, run:

```
require('ansi-html')('\x1b[0m\x1b[' + '0'.repeat(35))
```

Notice that node hangs at 100% CPU. Increasing the number of spaces increases the processing time.

On my laptop that would take three minutes to complete, whereas

```
require('ansi-html')('\x1b[0m\x1b[' + '0'.repeat(53))
```

would take just over **one year** to complete.

REMEDIATION

Remove the asterisk from the regular expression on line 62.

=

Doyensec (www.doyensec.com) is an independent security research and development company focused on vulnerability discovery and remediation. We work at the intersection of software development and offensive engineering to help companies craft secure code.

Copyright 2021 by Doyensec LLC. All rights reserved.

Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except by reformatting it, and that due credit is given. Permission is explicitly given for insertion in vulnerability databases and similar, provided that due credit is given. The information in the advisory is believed to be accurate at the time of publishing based on currently available information, and it is provided as-is, as a free service to the community by Doyensec LLC. There are no warranties with regard to this information, and Doyensec LLC does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

👍 24 🗨️ 7

krishnaUIDev commented on Jul 9, 2021

Looks like this package is not accepting new merge requests and not in maintenance 😞

🔗 [neil-gok](#) mentioned this issue on Jul 29, 2021

ReDoS Vulnerability webpack/webpack-dev-server#3576

Closed

2 tasks

SymbioticKilla commented on Aug 23, 2021

@Tjatse @glenjamin @danfuzz Any chance to fix this issue?

glenjamin commented on Aug 23, 2021

Contributor

I am not a maintainer of this project.

danfuzz commented on Aug 23, 2021

Contributor

Me neither, sorry!

graniczny commented on Aug 25, 2021

+1 any chance of fixing it @Tjatse ?

b-c-ds changed the title Exponential ReDoS Exponential ReDoS (CVE-2021-23424) on Aug 25, 2021

This was referenced on Aug 31, 2021

fix: limit backtracking exposure CVE-2021-23424 #20

Merged

fix: limit backtracking exposure CVE-2021-23424 gebhardtr/ansi-html#1

Merged

mahdyar added a commit to mahdyar/ansi-html-community that referenced this issue on Sep 5, 2021

fix: fix Tjatse#19

283cda2

mahdyar commented on Sep 5, 2021 • edited

Okay, I published the fixed version to npm. It's called [ansi-html-community](#) .
The repo: [@mahdyar/ansi-html-community](#) .

19

6

rap2hpoutre mentioned this issue on Sep 7, 2021

fix: replace ansi-html with ansi-html-community pmmmwh/react-refresh-webpack-plugin#501

Merged

pedantic79 mentioned this issue on Sep 9, 2021

ReDoS Vulnerability webpack-contrib/webpack-hot-middlewre#412

Closed

nttibbetts added a commit to nttibbetts/webpack-hot-middlewre that referenced this issue on Sep 9, 2021

replace ansi-html with ansi-html-community to fix vulnerability

9d41a29

nttibbetts added a commit to nttibbetts/webpack-hot-middlewre that referenced this issue on Sep 9, 2021

replace ansi-html with ansi-html-community to fix vulnerability

36ec7ba

nttibbetts added a commit to nttibbetts/webpack-hot-middlewre that referenced this issue on Sep 9, 2021

replace ansi-html with ansi-html-community to fix vulnerability

aaf2a6f

nttibbetts added a commit to nttibbetts/webpack-hot-middlewre that referenced this issue on Sep 9, 2021

fix: replace ansi-html with ansi-html-community to fix vulnerability

adeeade

nttibbetts mentioned this issue on Sep 9, 2021

fix: replace ansi-html with ansi-html-community to fix vulnerability webpack-contrib/webpack-hot-middlewre#413

Merged

6 tasks

danmarshall mentioned this issue on Sep 14, 2021

Replace ansi-html with ansi-html-community parcel-bundler/parcel#6899



chore(deps): Bump ansi-regex and replace ansi-html iTwin/iTwinUI-react#350



ty @mahdyar

If you're using yarn and this package is not a direct dependency of your repo, you can resolve this issue with [Selective Dependency Resolutions](#)

```
yarn add ansi-html-community@0.0.8
```

This instructs yarn to install `ansi-html-community@0.0.8` instead of `ansi-html`.

Confirmation

👍 23 ❤️ 3

0.0.7 is Vulnerable #21



ty @mahdyar

If you're using `yarn` and this package is not a direct dependency of your repo, you can resolve this issue with [Selective Dependency Resolutions](#)

```
yarn add ansi-html-community@0.0.8
```

This instructs yarn to install `ansi-html-community@0.0.8` instead of `ansi-html`.

After removing and re-installing node_modules (`rm -rf node_modules; yarn`) you can confirm that your `ansi-html` dependency is actually `ansi-html-community`

```
> cat node_modules/ansi-html/package.json
{
  "name": "ansi-html-community",
  "version": "0.0.8",
  "description": "An elegant lib that converts the chalked (ANSI) text to HTML. (Community)",
  "main": "index.js",
  "scripts": {
    "test": ".,/node_modules/.bin/mocha -R spec -t 5000"
```

```
    },
    "bin": {
      "ansi-html": "./bin/ansi-html"
    },
    "repository": {
      "type": "git",
      "url": "git://github.com/mahdyar/ansi-html-community.git"
    },
  },
  /* ... truncated ... */
```

Anyone know how to do this with [npm-force-resolutions](#)?

 **Brunarspunar** added a commit to `navikt/forebygg-sykefravaer` that referenced this issue on Oct 7, 2021

 Byttet ut ansi-html med ansi-html-community ...

e4caf24

CoryDanielson commented on Oct 7, 2021

@cmacdonnacha you may want to open an issue with npm-force-resolutions. I don't see anything in their docs for a resolution value that is not a version number.

- <https://github.com/rogeriochaves/npm-force-resolutions/issues>

cmacdonnacha commented on Oct 7, 2021

@cmacdonnacha you may want to open an issue with npm-force-resolutions. I don't see anything in their docs for a resolution value that is not a version number.

- <https://github.com/rogeriochaves/npm-force-resolutions/issues>


Thanks. It's actually CRA that uses this and they seem to have gone a but stale with releases so I think I will probably move to Vite.

  **GoryMoon** mentioned this issue on Oct 12, 2021

Replace ansi-html with ansi-hmtl-community GoryMoon/SubscriptionWhitelist#40

 Closed

 **aruniverse** added a commit to `imodeljs/create-react-app` that referenced this issue on Oct 13, 2021

 fix [cve-2021-23424](#), see [pmmwh/react-refresh-webpack-plugin#501](#) and [T...](#) ...

✗ e222fb4

  **aruniverse** mentioned this issue on Oct 13, 2021

Fix CVE 2021 23424 imodeljs/create-react-app#56

 Merged

  **jmthibault79** mentioned this issue on Oct 14, 2021

[risk=low][no ticket] replace the vulnerable + abandoned ansi-html with ansi-html-community all-of-us/workbench#5756

 Merged

 8 tasks

jdehorty commented on Oct 15, 2021 • edited

Anyone know how to do this with [npm-force-resolutions](#)?

@cmacdonnacha

As it turns out, `yarn` is not necessary. This is how you can do it using only `npm-force-resolutions` :

<https://stackoverflow.com/questions/69548370/how-to-override-a-nested-npm-sub-dependency-with-a-different-package-altogether/69591894#69591894>

 2  2  2

  **vkpraveen** mentioned this issue on Oct 18, 2021

ANSI-HTML is vulnerable and unmaintained facebook/create-react-app#11504

 Open

cmacdonnacha commented on Oct 18, 2021

Anyone know how to do this with [npm-force-resolutions](#)?

@cmacdonnacha As it turns out, `yarn` is not necessary. This is how you can do it using only `npm-force-resolutions` :

<https://stackoverflow.com/questions/69548370/how-to-override-a-nested-npm-sub-dependency-with-a-different-package-altogether/69591894#69591894>

That worked for me, thanks so much @jdehorty

 1

  **gileswells** mentioned this issue on Oct 22, 2021

API-3737 - Fix npm package audit issues department-of-veterans-affairs/developer-portal#898

 Merged

 6 tasks

ty @mahdyar

How to fix, if you're using yarn

If you're using yarn and this package is not a direct dependency of your repo, you can resolve this issue with [Selective Dependency Resolutions](#)

Install ansi-html-community

```
yarn add ansi-html-community@0.0.8
```

Add the resolution to your package.json

This instructs yarn to install `ansi-html-community@0.0.8` instead of `ansi-html`.

```
"resolutions": {
  "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz#69fbc4d6ccbe383f9736934ae34c3f8290f1bf41",
}
```

Confirmation

After removing and re-installing `node_modules` (`rm -rf node_modules; yarn`) you can confirm that your `ansi-html` dependency is actually `ansi-html-community`

```
> cat node_modules/ansi-html/package.json
{
  "name": "ansi-html-community",
  "version": "0.0.8",
  "description": "An elegant lib that converts the chalked (ANSI) text to HTML. (Community)",
  "main": "index.js",
  "scripts": {
    "test": "./node_modules/.bin/mocha -R spec -t 5000"
  },
  "bin": {
    "ansi-html": "./bin/ansi-html"
  },
  "repository": {
    "type": "git",
    "url": "git://github.com/mahdyar/ansi-html-community.git"
  },
  /* ... truncated ... */
}
```

This works. However, when I run `yarn audit` after making these changes, I receive this error:

```
An unexpected error occurred: "Unexpected audit response (Missing Metadata): false".
```

The project compiles and running this command `cat node_modules/ansi-html/package.json` gives the expected output of `ansi-html` being inferred as `ansi-html-community`. But, `yarn audit` fails with a 400 error response from npm.

Anyone facing this issue? Any solutions?



ty @mahdyar

How to fix, if you're using yarn

If you're using yarn and this package is not a direct dependency of your repo, you can resolve this issue with [Selective Dependency Resolutions](#)

Install ansi-html-community

```
yarn add ansi-html-community@0.0.8
```

Add the resolution to your package.json

This instructs yarn to install `ansi-html-community@0.0.8` instead of `ansi-html`.

```
"resolutions": {
  "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz#69fbc4d6ccbe383f9736934ae34c3f8290f1bf41",
}
```

Confirmation

After removing and re-installing `node_modules` (`rm -rf node_modules; yarn`) you can confirm that your `ansi-html` dependency is actually `ansi-html-community`

```
> cat node_modules/ansi-html/package.json
{
  "name": "ansi-html-community",
  "version": "0.0.8",
  "description": "An elegant lib that converts the chalked (ANSI) text to HTML. (Community)",
  "main": "index.js",
  "scripts": {
    "test": "./node_modules/.bin/mocha -R spec -t 5000"
  },
  "bin": {
    "ansi-html": "./bin/ansi-html"
  },
  "repository": {
    "type": "git",
    "url": "git://github.com/mahdyar/ansi-html-community.git"
  },
  /* ... truncated ... */
}
```

```
  },  
  /* ... truncated ... */
```

Thanks @mahdyar . This fix works and npm install works fine. However when I do "npm audit fix", I am seeing the below error.

```
$ npm audit fix  
npm ERR! Invalid Version: https://registry.npmjs.org/ansi-html-community/-/ansi-html-community-0.0.8.tgz
```

Could you check what's missing?

ShanUSAC commented on Oct 29, 2021

ty @mahdyar

How to fix, if you're using yarn

If you're using yarn and this package is not a direct dependency of your repo, you can resolve this issue with [Selective Dependency Resolutions](#)

Install ansi-html-community

```
yarn add ansi-html-community@0.0.8
```

Add the resolution to your package.json

This instructs yarn to install `ansi-html-community@0.0.8` instead of `ansi-html` .

```
"resolutions": {  
  "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz#69fbc4d6ccbe383f9736934ae34c3f8290f1b41",  
}
```

Confirmation

After removing and re-installing node_modules (`rm -rf node_modules; yarn`) you can confirm that your `ansi-html` dependency is actually `ansi-html-community`

```
> cat node_modules/ansi-html/package.json  
{  
  "name": "ansi-html-community",  
  "version": "0.0.8",  
  "description": "An elegant lib that converts the chalked (ANSI) text to HTML. (Community)",  
  "main": "index.js",  
  "scripts": {  
    "test": "./node_modules/.bin/mocha -R spec -t 5000"  
  },  
  "bin": {  
    "ansi-html": "./bin/ansi-html"  
  },  
  "repository": {  
    "type": "git",  
    "url": "git://github.com/mahdyar/ansi-html-community.git"  
  },  
  /* ... truncated ... */
```

Thanks @mahdyar . This fix works and npm install works fine. However when I do "npm audit fix", I am seeing the below error.

```
$ npm audit fix  
npm ERR! Invalid Version: https://registry.npmjs.org/ansi-html-community/-/ansi-html-community-0.0.8.tgz
```

Could you check what's missing?

My resolutions:

```
"resolutions": {  
  "browserslist": "4.16.5",  
  "dns-packet": "5.2.2",  
  "glob-parent": "6.0.1",  
  "url-parse": "1.5.2",  
  "path-parse": "1.0.7",  
  "jszip": "3.7.0",  
  "ansi-html": "https://registry.npmjs.org/ansi-html-community/-/ansi-html-community-0.0.8.tgz"  
},
```

jdehorty commented on Oct 29, 2021

@ShanUSAC are you trying to use yarn or npm?

If npm follow the directions outlined here:

<https://stackoverflow.com/a/69591894/12649786>

Note that you will also need a `preinstall` entry under scripts for that to work like this:

```
"scripts": {  
  "preinstall": "npx npm-force-resolutions",  
  "start": "react-scripts start",  
  "build": "react-scripts build",  
  "test": "react-scripts test --env=jsdom",  
  "eject": "react-scripts eject"  
}
```

kpeters-cbsi commented on Nov 9, 2021

ty @mahdyar

How to fix, if you're using yarn

If you're using yarn and this package is not a direct dependency of your repo, you can resolve this issue with [Selective Dependency Resolutions](#)

Install ansi-html-community

```
yarn add ansi-html-community@0.0.8
```

Add the resolution to your package.json

This instructs yarn to install `ansi-html-community@0.0.8` instead of `ansi-html`.

```
"resolutions": {
  "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz#69fbc4d6ccbe383f9736934ae34c3f8290f1bf41",
}
```

Confirmation

After removing and re-installing `node_modules` (`rm -rf node_modules; yarn`) you can confirm that your `ansi-html` dependency is actually `ansi-html-community`

```
> cat node_modules/ansi-html/package.json
{
  "name": "ansi-html-community",
  "version": "0.0.8",
  "description": "An elegant lib that converts the chalked (ANSI) text to HTML. (Community)",
  "main": "index.js",
  "scripts": {
    "test": "./node_modules/.bin/mocha -R spec -t 5000"
  },
  "bin": {
    "ansi-html": "./bin/ansi-html"
  },
  "repository": {
    "type": "git",
    "url": "git://github.com/mahdyar/ansi-html-community.git"
  },
  /* ... truncated ... */
}
```

I tried this with yarn in my project with two workspaces, `frontend` and `backend`. The `ansi-html` package is a dependency from something in the `frontend` workspace. I first tried adding the fix to `frontend/package.json`, but, while this produced no errors, `cat frontend/node_modules/ansi-html/package.json` still showed version `0.0.7`. So I tried adding the fix to the root `package.json`, but after I did `rm -rf node_modules frontend/node_modules backend/node_modules; yarn` I got:

```
→ locust-self-service git:(fix-cve-2021-23424) X rm -rf node_modules frontend/node_modules backend/node_modules; yarn; cat frontend/node_modules/ansi-html/package.json
> YN0000: Project validation
> YN0057: | frontend: Resolutions field will be ignored
> YN0000: | Completed
> YN0000: | Resolution step
> YN0001: | Error: ansi-html@https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz#69fbc4d6ccbe383f9736934ae34c3f8290f1bf41 isn't supported by any available resolver
    at Xc.getResolverByDescriptor (/Users/cpete0624/work/locust-self-service/.yarn/releases/yarn-3.0.2.cjs:294:5330)
    at Xc.bindDescriptor (/Users/cpete0624/work/locust-self-service/.yarn/releases/yarn-3.0.2.cjs:294:4719)
    at reduceDependency (/Users/cpete0624/work/locust-self-service/.yarn/releases/yarn-3.0.2.cjs:294:3379)
    at co.reduceHook (/Users/cpete0624/work/locust-self-service/.yarn/releases/yarn-3.0.2.cjs:295:3206)
    at p (/Users/cpete0624/work/locust-self-service/.yarn/releases/yarn-3.0.2.cjs:303:6768)
    at async Promise.all (index 65)
> YN0000: | Completed
> YN0000: Failed with errors in 0s 192ms
```

kdblocher commented on Nov 16, 2021

If you are using yarn and `ansi-html` is only a *transitive* dependency, you shouldn't need to install it yourself. Just using

```
"resolutions": {
  "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz",
}
```

should be enough.



kpeters-cbsi commented on Nov 16, 2021

If you are using yarn and `ansi-html` is only a *transitive* dependency, you shouldn't need to install it yourself. Just using

```
"resolutions": {
  "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz",
}
```

should be enough.

Do I put that in my root `package.json` or in `frontend/package.json`?



sauldeleon commented on Nov 18, 2021

worked like a charm. Thanks a lot @mahdyar

kdblocher commented on Nov 18, 2021

Whichever package.json is transitively referencing ansi-html. Look at the generated lockfile.
...

DeeDeeG added a commit to DeeDeeG/refugerestrooms that referenced this issue on Nov 27, 2021

deps: Resolve ansi-html to ansi-html-community ...

fd9b6d2

lomky mentioned this issue on Nov 30, 2021

Adds ansi-html-community to resolve abandoned ansi-html vulnerability cagov/ui-claim-tracker#565

→ Merged

1 task

bexsoft mentioned this issue on Dec 9, 2021

Updated ansi-html dependency to fix CVE vulnerability minio/console#1311

→ Merged

OxJem mentioned this issue on Jan 2

Fix ansi-html vulnerability OlympusDAO/olympus-frontend#1049

→ Merged

gonadarian mentioned this issue on Jan 5

vulnerable package version of custom-webpack being used inside build-angular for v12 angular/angular-cli#22433

⏸ Closed

digitaldogsbody added a commit to datacite/bracco that referenced this issue on Jan 28

Replace ansi-html with ansi-html-community (Tjatse/ansi-html#19)

151f4c6

Yonet commented on Feb 22

For those of you who are using npm:

How to fix, if you're using npm

Starting with [npm 8.3](#), you can add an option to override your dependency of your dependencies by defining overrides on your root package.json.

1. Override ansi-html with ansi-html-community in package.json
"overrides": { "ansi-html": "https://registry.yarnpkg.com/ansi-html-community/-/ansi-html-community-0.0.8.tgz" },
2. Delete your package-lock.json and node modules folder
3. npm install
npm i

👍 2

Tjatse closed this as completed in #20 on Feb 28

mahdyar mentioned this issue on Mar 17

Can't resolve 'ansi-html' in './node_modules/webpack-dev-server/client' mahdyar/ansi-html-community#10

⏸ Open

Abdul1110 mentioned this issue on May 11

CVE-2021-23424 @ Npm-ansi-html-0.0.7 Abdul1110/TEST_ORION#13

⏸ Open

Assignees

No one assigned

Labels

None yet

Projects


None yet


Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **fix: limit backtracking exposure CVE-2021-23424**
gebhardtr/ansi-html

 **fix: limit backtracking exposure CVE-2021-23424**
gebhardtr/ansi-html

16 participants

