

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

## Zalgo issue with v1.4.44-liberty-2 release #285

[Open](#)

Marak opened this issue on Jan 7 · 301 comments

Marak commented on Jan 7

[Owner](#)

It's come to our attention that there is a zalgo bug in the v1.4.44-liberty-2 release of colors.

Please know we are working right now to fix the situation and will have a resolution shortly.



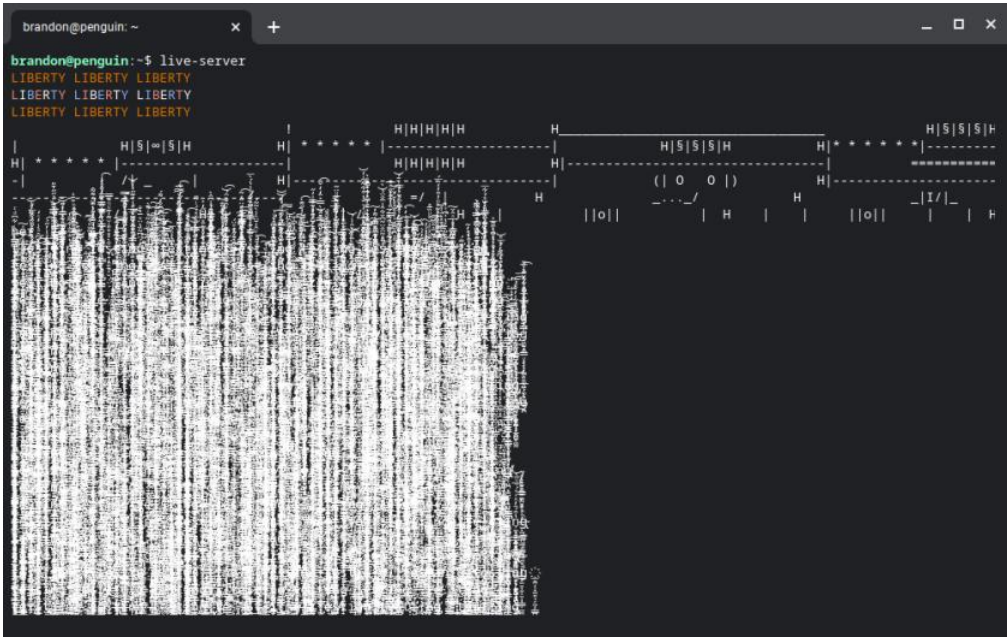
👍 153 🙌 221 🤔 116 [All reactions](#)

[📌](#) [Marak](#) pinned this issue on Jan 8

Offroaders123 commented on Jan 8

Woah, crazy bug! Glad to know you are working on it.

Just reinstalled the Live Server package because I came across this while trying to host a project over localhost. Tracked my way to the new `american.js` file here in your project because something related to this issue happened while starting the server. Really freaked me out! 🤪



👍 29 🗨️ 53

Offroaders123 commented on Jan 8

Alright, figured out how to temporarily fix the issue for use with Live Server.  
The `package.json` for Live Server has `Colors.js` set to use the newest possible version available, `latest`, so I changed it back to the most recent `Colors.js` version that didn't have the issue, `1.4.0`.  
Just thought I'd share a fix for anyone else that may also run into this too 🙌

👍 25

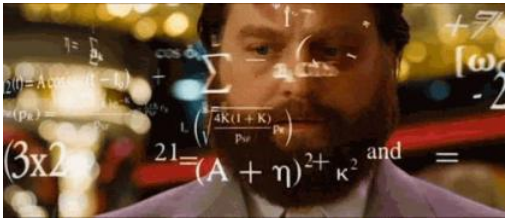
niknrb commented on Jan 8

👋 Hi  
Seems like it was introduced because of [this](#) infinite loop

👍 20 🗨️ 4 😬 5

Marak commented on Jan 8

Owner Author



Still trying to figure out what happened. I think we may have tried to upgrade to JavaScript 6 but the CI system only supports JavaScript 5 and lower.

👍 13 🙌 87 🗨️ 77 [All reactions](#)

legendary0001 commented on Jan 8





👍 7 🙌 2 🗨️ 107


🔗 [SimenB](#) mentioned this issue on Jan 8

Jest (or Rollup) ecosystem dependency hacked? [facebook/jest#12226](#)

🔒 Closed

  **christiansmith** mentioned this issue on Jan 8

**Package appears to be compromised.** [oclif/oclif#786](#)

 Closed

**Offroaders123** commented on Jan 8

Is it an option that, in the meantime, you could revert your project back to `1.4.0`, the release before the new change was introduced? This seemed to fix all of the issues on my end. A lot of large projects appear to be requiring your dependency, and they have the version number set to use the `latest` release.

 4

**Marak** commented on Jan 8 • edited ▾

**Owner** **Author**



We've been up all night trying to work out a solution for this Zalgo bug and are still coming up short.

As much as we'd like to revert back to a previous working version, we strongly feel it's best if we can fix the actual problem instead of going back in time.



<https://www.youtube.com/watch?v=KEkrWRHCDQU>

 44  43  37  2

**Offroaders123** commented on Jan 8 • edited ▾

Yeah, changing the version number to an older release would fix it, but there are many projects out there that haven't been updated in multiple years, I don't think the devs for them will be around to change the Colors.js dependency not to use `latest` any time soon, [Live Server](#) could be an example. (This message was in reply to [this one above](#))

 3

**mdonnanley** commented on Jan 8 • edited ▾

@**Marak** can you please promote the last working version to latest? I understand that you'd rather fail forward but our package is completely unusable because of this bug

 8  11

Marak commented on Jan 8 • edited

Owner Author



I'm all out of ideas here. It's been a long night and I do I have to begin to prepare soup for Sunday church services tomorrow. I'll try to come back to this Monday if time permits.

Perhaps one of other maintainers can assist?

@substack @dominictarr and @tj should all have publishing access to NPM.

👍 23 🍷 31 🍌 11 🗣️ 3 ❤️ 7 🚩 9

DABH commented on Jan 8

Contributor

@Marak, It looks like you removed me from this repo so I'm unable to help. I can only imagine everything you're going through right now, but there are a bunch of other OSS devs like you who get hurt by pranks like this, rather than the big tech elite etc. that I think you are trying to go after. I'd be happy to help here, but please be willing to not harm the folks who would otherwise be on your side.

👍 316 🍷 6 ❤️ 66

Darker-Ink commented on Jan 8

Best Bug though. You for sure should keep it in 🍷 makes the console look cooler in my opinion.

👍 47 🍌 22 🗣️ 9 ❤️ 7 🚩 7

🔗 championfelliin mentioned this issue on Jan 8

**cdk-cli: cannot deploy due to colors dependency** aws/aws-cdk#18322

🔒 Closed

nbarikopoulos commented on Jan 8

In package-lock file we trust and I will trust even for simple project...

👍 16 🍌 16

trusktr commented on Jan 8 • edited

Hello whoever is behind this Marak account. Imagine if you turned your skill into making products for average humans that don't code, to improve their lives in big ways, leaving a bigger and longer lasting memory of what you've done... Bombs won't have as big of an impact in today's world.

👍 21 🍷 15 ❤️ 18 🚩 3

🔗 nbarikopoulos mentioned this issue on Jan 8

**Fix issue with the colors module** nbarikopoulos/wix-msi#23

🔒 Closed

heisian commented on Jan 8



👍 11 ❤️ 4

🔗 enderandpeter mentioned this issue on Jan 8


**Project may have been compromised. Large amount of ASCII art instead of lesson** workshopper/javascripting#327

🔒 Closed


🔗 DanielRuf mentioned this issue on Jan 8

**heads up: broken colors package** itgalaxy/favicons#370

🔒 Closed

 **p1mwd** mentioned this issue on Jan 8

(cli): liberty liberty liberty? aws/aws-cdk#18323

 Closed

**DanielRuf** commented on Jan 8 • edited

For anyone who is affected, here are ways to check, which packages have to pin the version (the ones which directly use colors):

for npm:

```
npm ls colors
```

for yarn:

```
yarn why colors
```

In some cases you can use resolutions:

<https://classic.yarnpkg.com/lang/en/docs/selective-version-resolutions/>

<https://www.npmjs.com/package/npm-force-resolutions>

And in some you can easily apply a patch to remove the relevant code parts with patch-package: <https://www.npmjs.com/package/patch-package>

 38  1

**timleg002** commented on Jan 8

Or check one technology called Haskell; you could even write pure (determined) IOs using one thing called Monads 🤖 It's big fun Then you could run code that never ever break, having a one century of technology under your fingertips would then be possible look how <https://negativespace.co/iphone-woman-hands-touch/>

all haskell evangelists are now rust evangelists, youre stuck in time bro

 21  23

**cinderblock** commented on Jan 8

What are we, the confused internet, missing here? What's going on? Is this some sort of April Fools' joke? Are you trying to get developers to not use @latest tags when installing dependencies?

**sbmelvin** commented on Jan 8

So has a successor to colors.js been decided yet?

 1

**cinderblock** commented on Jan 8

@DanielRuf Yeah, I'm not going to go sleuthing around trying to find the relevant story. A lot just point back here but all I see are what look like inside jokes. Thank you for the HN link.

I see that faker.js is related but it looks like the original post the HN post is about has been deleted along with the repository. I've got to go back to the Way Back Machine to get some details:

<https://web.archive.org/web/20210704022108/https://github.com/Marak/faker.js/issues/1046>

@sbmelvin I like chalk

 **mceachen** mentioned this issue on Jan 8

"Zalgo" bomb from dependency on the "colors" package npkgz/cli-progress#116

 Closed

**slavanomics** commented on Jan 8

absolute legend for this thank you marak dont let anyone tell you otherwise

 34  51  6  4

437 hidden items

[Load more...](#)

**renhiyama** commented on Jan 14

And now I am both in support and against Marak.

Summing up total about whatever comments I have read here. Marak definitely made fortune companies notice him and his work. Can we just learn this fact: When this zalgo thingy never came, nobody knew Marak. Honestly. But he was a building pillar of such a big community. But 3 days ago, we all are now noticing him about his bad deeds. Can't we ask him a sorry for once? I think it's not right to say "fuck off Marak" to him because we never thanked him in the first place.

Now, against: as pointed out by someone above, an eg: doctor could have cancelled so many appointments, and so many patients could have died due to this... This way was definitely not the correct way to raise awareness... But this way DID raised awareness, I have seen countless blogs and news about Marak now, including Snyk blogs too. He has written history, but not in golden letters, but in black dark letters. Sorry Marak. Open source is not the way to go if you want to earn for a living

 13  1  3

notwedtm commented on Jan 14

And now I am both in support and against Marak. Summing up total about whatever comments i have read here. Marak definitely made fortune companies notice him and his work. Can we just learn this fact: When this zalgo thingy never came, nobody knew Marak. Honestly. But he was a building pillar of such a big community. But 3 days ago, we all are now noticing him about his bad deeds. Can't we ask him a sorry for once? I think it's not right to say "fuck off Marak" to him because we never thanked him in the first place.

Now, against: as pointed out by someone above, an eg: doctor could have cancelled so many appointments, and so many patients could have died due to this... This way was definitely not the correct way to raise awareness... But this way DID raised awareness, I have seen countless blogs and news about Marak now, including Snyk blogs too. He has written history, but not in golden letters, but in black dark letters. Sorry Marak. Open source is not the way to go if you want to earn for a living

You are absolutely correct. The fact that **@Marak** took this approach should not "cancel" his massive contributions to the open-source community. It is sad and unfortunate that he did not receive accolades appropriate to his contributions, and that should absolutely be addressed.

Voluntarily contributing to open source is not a requirement. Likewise, doing so with an *expectation* of surviving and living off of it is a very risky approach. Should there be a more concerted effort to provide financial stability to these contributors? Absolutely. Was there ever a guarantee or a promise that was made and not kept to do so? No.

Some places exist already to close the gap in this regard. Places like [opencollective.org](https://opencollective.com/marak), which shows that **@Marak** has received a not-insignificant amount for his work. (<https://opencollective.com/marak>)

Should it be more? Almost certainly.

Does it justify what was done? Absolutely not.

Did **@Marak** really do anything to those mega corps that he has been slighted by? No. They did exactly what everyone else in this thread has suggested, forked the repo, and moved on. It wasn't even a blip on their radar.

👍 14

hello-smile6 commented on Jan 14

If someone wants to tarnish his reputation and burn all his work to JUST MAKE A POINT, more power to him. Now his action is felt cross the tech community and beyond. People and corporations now need to think twice before using open source stuff. What are the underlying problems his action showed us?

1. It is hard to make a comfortable income with open source.
2. Big corporations profit from open source projects and pay so little. (Apple sent tech-support inquiry from its paying customer to Curl, a open source project)
3. I never needed to know who made my life easy by providing their code for free. I never needed to pay or thanked them. I just needed the code to work. Am I in the minority?

People knew about the problems. Now more people are aware of the problems at the expense of Marak REGARDLESS of his intention. Yes, it caused some people some inconvenience. Those individual inconvenience is no way equal to Marak's. What about the collective inconvenience of the entire tech community he caused? So the collective convenience of his work never yielded him enough money and now he SHOULD BE held accountable?

I think many "Zalgo" were bound to happen. And it happened. A solution or not, the tech landscape is a bit different now thanks or "thanks" to Marak's action.

They did the right thing.

👍 5 🙌 4 🍷 2 🚫 1 ❤️ 1 🗑️ 1 🗨️ 3

RoopanV commented on Jan 15 • edited

[#317 \(comment\)](#)

Requesting all folks to get handy with an alternative

hello-smile6 commented on Jan 15

[#317 \(comment\)](#)

Requesting all folks to get handy with an alternative

Are they planning to dOS people?

JoneKone commented on Jan 16

If you where an EU citizen you could request a forget my data.

👍 1

nukeop commented on Jan 16



## A Cuck Licenser gets what he deserves (and we all pay the price).

One of the funniest and saddest horror stories of Cuck Licenses I can think of is Andrew Tanenbaum, who released MINIX, an operating system, under a BSD license. Intel silently took this software (thanks to its license) and unbeknownst to him, used it for their Intel Management Engine, **making it the OS of the spyware microprocessor/backdoor now running in all Intel CPUs**. We all have a permanent NSA backdoor because of the Intel Management Engine—all made possibly my Cuck License cuckery.

Only many, many years later was this even revealed to Tanenbaum. Read that blog post of his as he slowly externalizes his mixed feelings, tinged with guilt. After all, on the "bright" side, he says:

"I guess that makes MINIX the most widely used computer operating system in the world, even more than Windows, Linux, or MacOS."

Wow, what a proud achievement. But regardless, Tanenbaum already feels some regret about the fact that his permissive license allowed Intel to withhold this:

"This was a complete surprise. I don't mind, of course, and was not expecting any kind of payment since that is not required. There isn't even any suggestion in the license that it would be appreciated.

"The only thing that would have been nice is that after the project had been finished and the chip deployed, that someone from Intel would have told me, just as a courtesy, that MINIX was now probably the most widely used operating system in the world on x86 computers. That certainly wasn't required in any way, but I think it would have been polite to give me a heads up, that's all."

You can feel the regret. **With Cuck Licenses, you get the worst of two worlds:** You get no credit for your work, nor money for licensing fees like other proprietary software and your software will be used to violate your and other users' privacy when it is used in closed-source environments. Oh, no... copes incoming:

"Many people (including me) **don't like the idea of an all-powerful management engine in there at all** (since it is a possible security hole and a dangerous idea in the first place), but that is Intel's business decision and a separate issue from the code it runs. A company as big as Intel could obviously write its own OS if it had to."  
*emphasis added*



👍 7 🗨️ 2

jerdoe commented on Jan 16

Many tell that Marak did hurt open source community with his last actions and has made people lost confidence in open source software. But does it not highlight on the contrary how open source is great and how much it can be trusted ?

Because source was opened, anyone could have it with its whole history of commits and could revert it back to its last working release !

Because of the license, many people used Marak libs for free and since it was so widely used, community minded giving some fixes to everyone (using a fork, or pinning the version). Some private entities felt also obliged to support the open source community ; NPM unreleased the broken version.

If from the start, these libs had closed sources, would it have been so popular ? Would have it got fixed that fast ? If the libs were stuck in the hands of a unique private entity, and assuming that someone working there had corrupted/removed all the work done, what would have happened to the users ?

However, one should take note that the code could be deliberately more malicious and damaging : developers using open source libraries should become better aware of good practices and users of open source softwares should understand that those are usually provided "as-is" (in spite of a fair amount of certitude that a solution will be provided if widely used by the community)

👍 18

pravindahal commented on Jan 16

@bacloud14 my friend, <https://github.com/bacloud14/Classified-ads-48/blob/main/package.json> does not do version pinning.

Instead of an infinite loop, what if @Marak had decided instead to simply start sending all data in your application to him? Would your tests catch that?

Looking at your repo specifically, it would be pretty easy for any of the authors of the packages you import to own you pretty quickly.

That repo does use package-lock.json, so there is no need for version pinning in package.json.

hello-smile6 commented on Jan 16

@bacloud14 my friend, <https://github.com/bacloud14/Classified-ads-48/blob/main/package.json> does not do version pinning.

Instead of an infinite loop, what if @Marak had decided instead to simply start sending all data in your application to him? Would your tests catch that?

Looking at your repo specifically, it would be pretty easy for any of the authors of the packages you import to own you pretty quickly.

That repo does use package-lock.json, so there is no need for version pinning in package.json.

People aren't taught to use `npm ci`. `npm ci` should be the default for `npm install`, the current behavior should require a flag.

👍 3

dustinlw1987 commented on Jan 17

@Marak just lost faker.js. The community has taken it from him and rightly so: <https://fakerjs.dev/update.html>

👍 3 🗳️ 1

hello-smile6 commented on Jan 17

| @Marak just lost faker.js. The community has taken it from him and rightly so: <https://fakerjs.dev/update.html>

They should've pulled back earlier.

renhiyama commented on Jan 17 • edited ▾

I trust @Marak still now, and will do in future! Don't dislike this comment you guys if you don't support him, it's my personal opinion and I have the right to support him, and he has the right to make and destroy codes. More happy because this method did SHAKE the whole social media and blogs, and his message to fortune companies definitely went to them!

The vast majority of "support" comes from anonymous accounts with little to no contributions to open source themselves. You have continued to shill and throw random support towards Marak with no understanding of what "trust" is.

You say you "trust" Marak still now. What do you "trust" him to do?

At this point, I'm convinced you are just an alt account of Marak's that being using to stir the pot.

Me? An alt? Oh I didn't know I had the chance to call myself such a popular person! Anyways I am the owner of @rovelstars org. Deal with it 🤔

And I'm a owner of @labdiscord. Most of us are owners of an organization. Humble yourself.. and what the hell is RovelStars anyways?

And what's LabDiscord?

🤔 Thanks for dealing with that guy. I myself posted my org to prove that I'm not an alt of Marak, and I don't care whether my organization is that popular or not, but it has a 120 stars repo, enough to prove that im not an alt of Marak. Labdiscord guy should have learnt about this instead of starting to promote his too without being asked to 🙄(〃〃)〃

👍 2 🗳️ 4

✉️ ThatRedPandaDev commented on Jan 18

You said deal with it as if you were flexing your organization and having a repo with stars doesn't prove you're not an alternate account of Marak.

Either way, I'm tired of losing brain cells on this issue (and I'm pretty sure everyone else is too) so I'm unsubscribing from here on. Good luck in life with your future endeavors.

...

🔗  gas1cent mentioned this issue on Jan 18

Downgrade colors.js to 1.4.0 defi-wonderland/solidity-hardhat-boilerplate#35

➡️ Merged



Taro-Naza commented on Jan 22

It's come to our attention that there is a zalgo bug in the v1.4.44-liberty-2 release of colors.

Please know we are working right now to fix the situation and will have a resolution shortly.



You're just childish! this is a pathetic behavior



StepanZharychev commented on Jan 23

So the long story short: guy published software under fully open license which allowed commercial usage, abandoned the project so other people supported it literally for years, project became very popular at some point, guy developed jealousy because it was non-profit and decided to break the project.

Except it's extremely unprofessional and childish behavior (it's not activism, fellow developers, because big companies wouldn't even notice it, since dependencies are on strict control there):

1. Marak fully mimicked behavior of "evil corps" by destroying 2 projects which were founded by him, yes, but maintained by many other people, basically saying "I own it and don't care about your efforts";
2. As it was said tons of times he could've changed licensing to non-commercial;

I'm deeply disappointed by this situation and happy to see that community now leads those projects.



azriel46d mentioned this issue on Feb 4

Latest version 4.4.15 utilises a compromised colors package vue-styleguidist/vue-styleguidist#1274

Closed

Saiv46 commented on Feb 5

Except it's extremely unprofessional and childish behavior (it's not activism, fellow developers, because big companies wouldn't even notice it, since dependencies are on strict control there):

Big companies would notice that by failing tests, and the shitstorm towards this package, otherwise GitHub wouldn't even block his account in first place (there's actual backdoored packages and just outdated packages with vulnerabilities).

1. Marak fully mimicked behavior of "evil corps" by destroying 2 projects which were founded by him, yes, but maintained by many other people, basically saying "I own it and don't care about your efforts";

That's the issue with OSS, ex. lead maintainer could crap your for your patch and that's it.

2. As it was said tons of times he could've changed licensing to non-commercial;

Then Big companies will just fork from previous version and then just make original package obsolete, that'll be undesirable for Marak.

I'm deeply disappointed by this situation and happy to see that community now leads those projects.

I'm disappointed by reaction of devs, that reminds me of the similarity of cancel culture and apostasy in islam.



Alex4386 added a commit to Alex4386/typescript-kickstart that referenced this issue on Feb 5

chore: mitigating issues from Marak/colors.js#285. ...

4ce41ef

rilysh commented on Feb 17

@Marak lmao c'mon dude, at least explain who "we" are as you've mentioned above.

  kylemh mentioned this issue on Mar 17

**Strange output from React-PropTypes-to-prop-types** reactjs/react-codemod#306

 Open

kuizeo commented on Jun 10

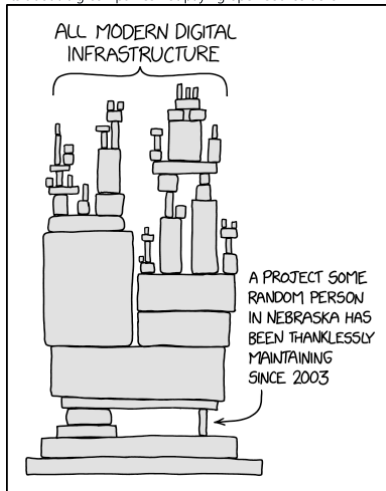
Looking at the date of this (January 7th), I assume this has something to do with the attacks on January 6th? The public hearing was today, so what a fitting time to say — fix this. Don't ruin your project because of your political opinions.

And if, by some chance, this is about something else? Fix it regardless.

 1

DumbGameMaker commented on Jun 11 • edited

Its about big companies not paying open source devs



 7

 This was referenced on Jul 10

**Remove security alerts** nbarikipoulos/wix-msi#31

 Closed

**Replace the colors.js package** nbarikipoulos/wix-msi#32

 Closed

**Replace the colors.js package** nbarikipoulos/poppy-robot-cli#72

 Closed

Crsarmv71 commented on Jul 29 • edited

So the long story short: guy published software under fully open license which allowed commercial usage, abandoned the project so other people supported it literally for years, project became very popular at some point, guy developed jealousy because it was non-profit and decided to break the project.

Except it's extremely unprofessional and childish behavior (it's not activism, fellow developers, because big companies wouldn't even notice it, since dependencies are on strict control there):

1. Marak fully mimicked behavior of "evil corps" by destroying 2 projects which were founded by him, yes, but maintained by many other people, basically saying "I own it and don't care about your efforts";
2. As it was said tons of times he could've changed licensing to non-commercial;

I'm deeply disappointed by this situation and happy to see that community now leads those projects.

I dislike this train of thought. If I own a house, but leave for a few years and someone lives there and maintains it, it is still MY house, not theirs.

(Although I know with the covid eviction moratoriums governments are actively trying to change that).


Others may have maintained the project but it is still marek's to do with what he wants...and he did. Most people here are just winners.

 1  1

kuizeo commented on Jul 31

this is a great way of analogizing it



 JuhG mentioned this issue on Oct 28

Colors package breaks CLI UXPin/uxpin-merge-tools#332

 Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

114 participants

