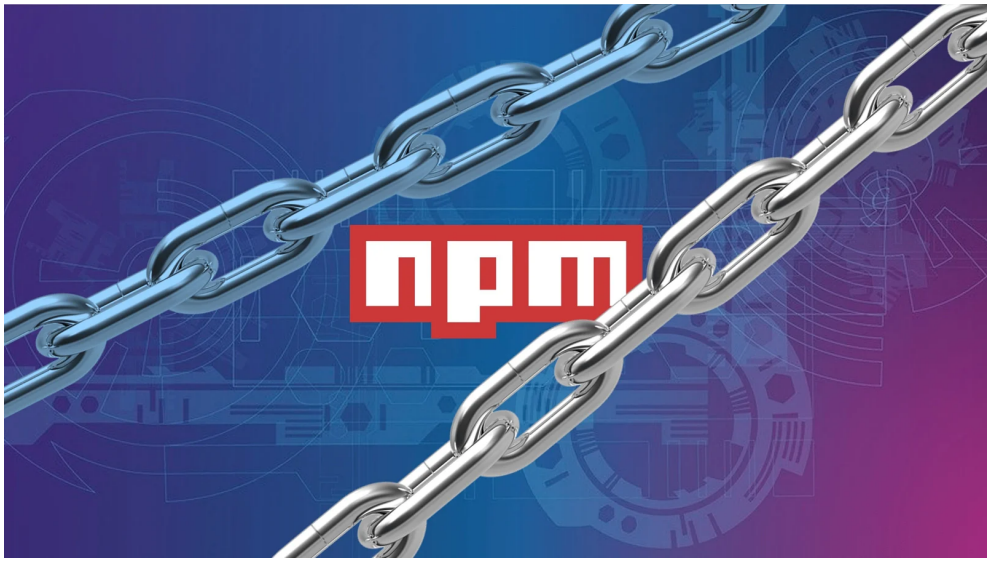
Dev corrupts NPM libs 'colors' and 'faker' breaking thousands of apps

By **Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)** January 9, 2022 09:17 AM 4



Users of popular open-source libraries 'colors' and 'faker' were left stunned after they saw their applications, using these libraries, printing gibberish data and breaking.

Some surmised if the NPM libraries had been compromised, but it turns out there's much more to the story.

The developer of these libraries intentionally introduced an infinite loop that bricked **thousands of projects** that depend on 'colors' and 'faker.'

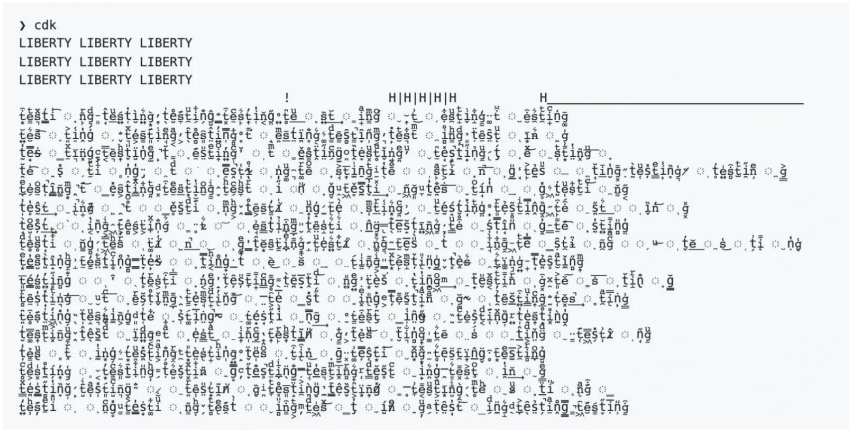
The *colors* library receives over 20 million weekly downloads (https://www.npmjs.com/package/colors) on npm alone and has almost 19,000 projects relying on it. Whereas, *faker (https://www.npmjs.com/package/faker)* receives over 2.8 million weekly downloads on npm, and has over 2,500 dependents.

Open Source Revolution?

The developer behind popular open-source NPM libraries 'colors' (aka colors.js on GitHub (https://github.com/Marak/colors.js)) and 'faker' (aka 'faker.js' on GitHub (https://github.com/marak/Faker.js/)) intentionally introduced mischievous commits in them that are impacting thousands of applications relying on these libraries.

Yesterday, users of popular open-source projects, such as Amazon's Cloud Development Kit (https://github.com/aws/aws-cdk/issues/18323) (aws-cdk) were left stunned on seeing their applications print gibberish messages on their console.

These messages included the text 'LIBERTY LIBERTY LIBERTY' followed by a sequence of non-ASCII characters:

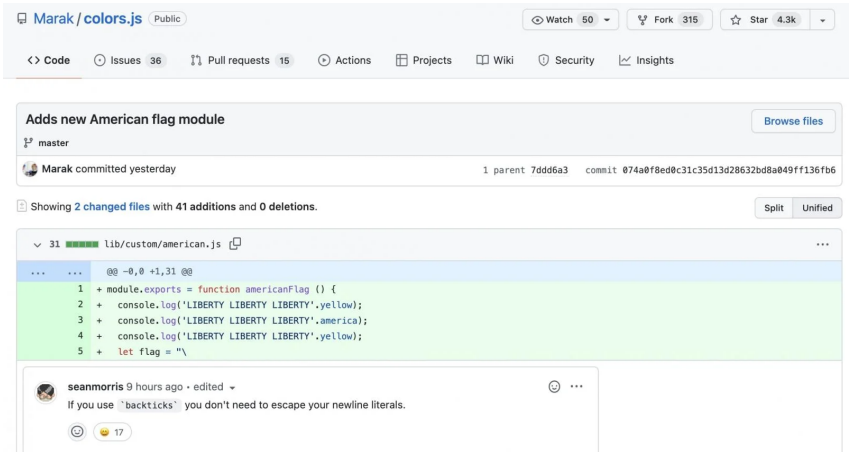


Users left stunned on seeing garbage data printed by 'faker' and 'colors' projects (GitHub)

Initially, users suspected that the libraries 'colors' and 'faker' used by these projects were compromised [1 (https://github.com/aws/aws-cdk/issues/18323), 2 (https://github.com/workshopper/javascripting/issues/327), 3 (https://github.com/oclif/oclif/issues/786)], similar to how coa, rc, (https://www.bleepingcomputer.com/news/security/popular-coa-npm-library-hijacked-to-steal-user-passwords/) and ua-parser-j (https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/)s libraries were hijacked last year by malicious actors.

But, in fact, it was the dev behind *colors* and *faker* who appears to have intentionally committed (https://github.com/Marak/colors.js/commit/074a0f8ed0c31c35d13d28632bd8a049ff136fb6?diff=unified) the code responsible for the major blunder, as seen by BleepingComputer.

The developer, named Marak Squires added a "new American flag module" to *colors.js* library yesterday in version *v1.4.44-liberty-2* that he then pushed to GitHub (https://github.com/Marak/colors.js/commit/6bc50e79eeaa1d87369bb3e7e608ebed18c5cf26) and npm.



colors.js mischievous commit made by 'Marak' (GitHub)

The infinite loop (https://github.com/Marak/colors.js/commit/074a0f8ed0c31c35d13d28632bd8a049ff136fb6#diff-92bbac9a308cd5fcf9db165841f2d90ce981baddcb2b1e26cfff170929af3bd1R18) introduced in the code will keep running indefinitely; printing the gibberish non-ASCII character sequence endlessly on the console for any applications that use 'colors.'

Likewise, a sabotaged version '6.6.6' of *faker* was published to (https://github.com/Marak/faker.js/blob/master/package.json#L4) Git Hub and npm.

"It's come to our attention that there is a zalgo bug in the v1.4.44-liberty-2 release of colors," mocked (https://github.com/Marak/colors.js/issues/285) the developer.

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

Zalgo text (https://www.bleepingcomputer.com/news/technology/why-certain-characters-glitch-gmail-youtube-and-twitter/) refers to certain non-ASCII characters that appear glitchy.

The reason behind this mischief on the developer's part appears to be retaliation—against mega-corporations and commercial consumers of open-source projects who extensively rely on cost-free and community-powered software but do not, according to the developer, give back to the community.

In November 2020, Marak had warned that he will no longer be supporting the big corporations with his "free work" and that commercial entities should consider either forking the projects or compensating the dev with a yearly "six figure" salary.

"Respectfully, I am no longer going to support Fortune 500s (and other smaller sized companies) with my free work. There isn't much else to say," the developer previously wrote (http://web.archive.org/web/20210704022108/https://github.com/Marak/faker.js/issues/1046).

"Take this as an opportunity to send me a six figure yearly contract or fork the project and have someone else work on it.

Interestingly, as of today, BleepingComputer noticed that the README (https://github.com/marak/Faker.js/) page for the 'faker' GitHub repo was also modified by the developer to make reference to Aaron Swartz (https://en.wikipedia.org/wiki/Aaron_Swartz) by stating: "What really happened with Aaron Swartz?"

Swartz was an American programmer, entrepreneur, and renowned hacktivist who, following a legal battle, committed suicide (https://www.eff.org/deeplinks/2013/01/farewell-aaron-swartz).

In an effort to make information freely accessible to all, the hacktivist downloaded millions of journal articles from the JSTOR database present on the MIT campus network, allegedly by rotating his IP and MAC addresses repeatedly to get around the technological blocks put in place by JSTOR and MIT.

In the process of doing this, Swartz may have run afoul of the Computer Fraud and Abuse Act and faced criminal charges, with penalties of up to thirty-five years in prison.

Uncanny can of worms

Marak's bold move has opened up a can of worms and attracted mixed responses.

Some members of the open-source software community have praised the developer's actions, while others are appalled by it.

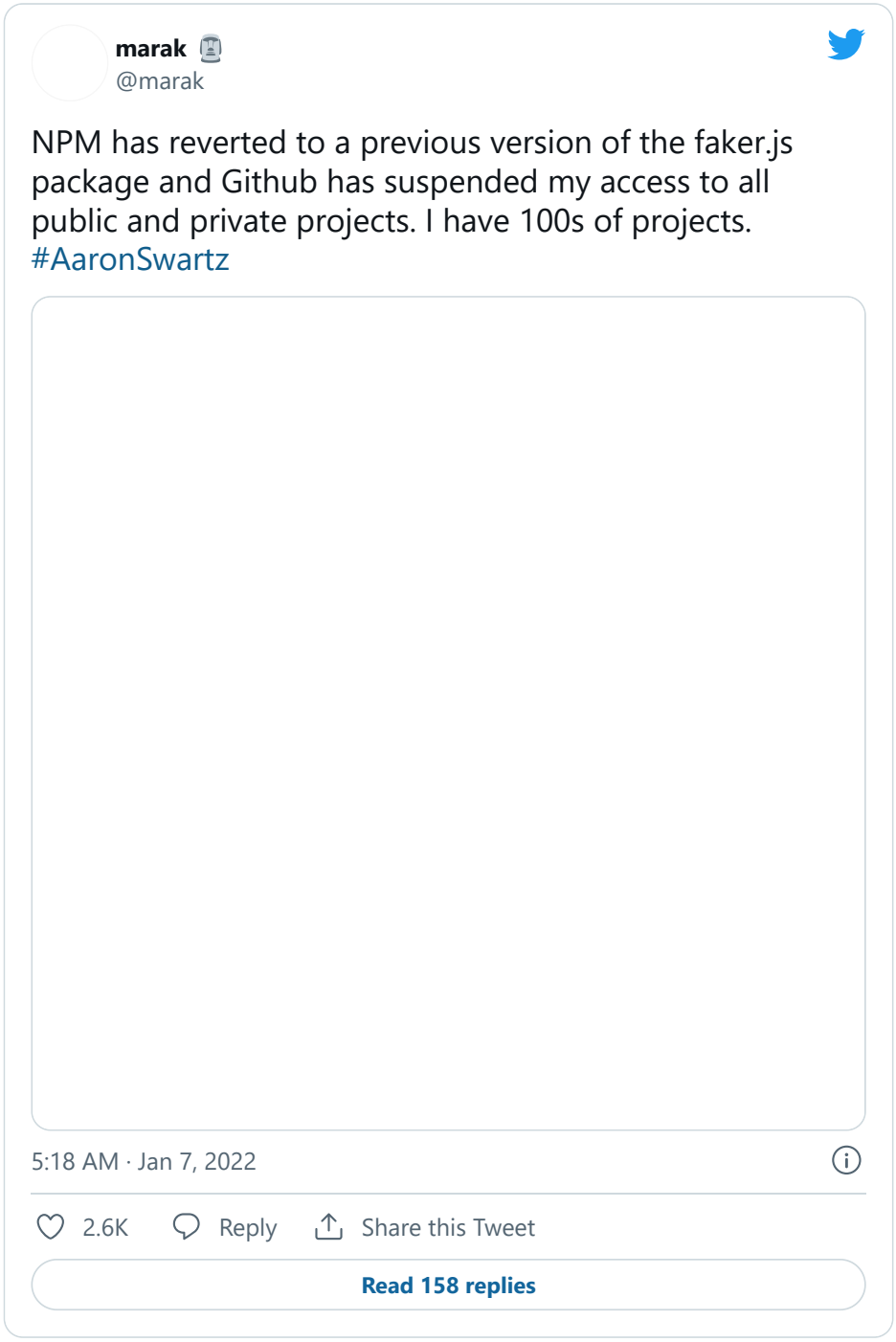
"Apparently the author of 'colors.js' is angry for not being payed... So he decided to print the American flag each time his library is loaded... WTF," tweeted (https://twitter.com/galtashma/status/1479929747337580546) one user.

Some dubbed (https://twitter.com/vaultec81/status/1479991084587499521) this an instance of "yet another OSS developer going rogue," whereas InfoSec

expert *VessOnSecurity* called the action "irresponsible (https://twitter.com/VessOnSecurity/status/1480189534625320960)," stating:

"If you have problems with business using your free code for free, don't publish free code. By sabotaging your own widely used stuff, you hurt not only big business but anyone using it. This trains people not to update, 'coz stuff might break."

GitHub has reportedly suspended the developer's account. And, that too, has caused mixed reactions:



"Removing your own code from [GitHub] is a violation of their Terms of Service? WTF? This is a kidnapping. We need to start decentralizing the hosting of free software source code," responded (https://twitter.com/sgomez/status/1480148595059965956) software engineer Sergio Gómez.

"Never know what happened but I'm hosting all of my projects on GitLab private instance just in cause things like this happening to me. Never trust any internet service provider," tweeted (https://twitter.com/Lakr233/status/1480178455736033282) another.

"Marak yeeted faker and colors, bricking tons of projects, and expected nothing to happen?" stated (https://twitter.com/piemadd/status/1480017317278978048) a developer named Piero.

Note, Marak's surprising move follows the recent Log4j debacle that set the internet on fire (https://www.bleepingcomputer.com/news/security/new-zero-day-exploit-for-log4j-java-library-is-an-enterprise-nightmare/).

Open-source library Log4j is used extensively in a vast range of Java applications, including those developed by corporations and commercial entities.

But, shortly after mass-exploitation of the Log4shell vulnerability, the maintainers of the open-source library worked without compensation over the holidays to patch the project, as more and more CVEs were being discovered (https://www.bleepingcomputer.com/news/security/all-log4j-logback-bugs-we-know-so-far-and-why-you-must-ditch-215/).

Concerns emerged as to how big businesses were used to "exploiting (https://www.theregister.com/2021/12/14/log4j_vulnerability_open_source_funding/)" open-source; by consuming it incessantly but not giving back enough to support the unpaid volunteers who sustain these critical projects by giving up their free time.

Some also criticized the netizens and bug bounty hunters hounding the Log4j maintainers who were already "working sleeplessly on mitigation measures; fixes, docs, CVE, replies to inquiries, etc." [1 (https://twitter.com/yazicivo/status/1469349956880408583), 2 (https://twitter.com/pentestscraps/status/1473707415635963919), 3 (https://twitter.com/GossiTheDog/status/1469848362325270530)].

"The responses to the colors.js/faker.js author sabotaging their own packages are really telling about how many corporate developers think they are morally entitled to open source developers' unpaid labour without contributing anything back," wrote (https://twitter.com/sadiekatze/status/1480164481112100872) one Twitter user.

Time will tell what the future of open-source software entails, with regards to the OSS sustainability problem (https://github.blog/2019-01-17-lets-talk-about-open-source-sustainability/).

In the meantime, users of 'colors' and 'faker' NPM projects should ensure they are not using an unsafe version. Downgrading to an earlier version of colors (e.g. 1.4.0) and faker (e.g. 5.5.3) is one solution.

Update 10:08 AM ET: Added tweet from @VessOnSecurity after publishing.

Update 11:24 AM ET: Added developer's full name, Marak Squires.

Related Articles:

NPM fixes private package names leak, serious authorization bug (https://www.bleepingcomputer.com/news/security/npm-fixes-private-package-names-leak-serious-authorization-bug/)

'Trojan Source' attack method can hide bugs into open-source code (https://www.bleepingcomputer.com/news/security/trojan-source-attack-method-can-hide-bugs-into-open-source-code/)

Hackers use video player to steal credit cards from over 100 sites (https://www.bleepingcomputer.com/news/security/hackers-use-video-player-to-steal-credit-cards-from-over-100-sites/)

All Log4j, logback bugs we know so far and why you MUST ditch 2.15 (https://www.bleepingcomputer.com/news/security/all-log4j-logback-bugs-we-know-so-far-and-why-you-must-ditch-215/)

Log4j 2.17.1 out now, fixes new remote code execution bug (https://www.bleepingcomputer.com/news/security/log4j-2171-out-now-fixes-new-remote-code-execution-bug/)