

Open source developer corrupts widely-used libraries, affecting tons of projects

A developer appears to have purposefully corrupted a pair of open-source libraries on GitHub and software registry npm – “faker.js” and “colors.js” – that thousands of users depend on, rendering any project that contains these libraries useless, as reported by *Bleeping Computer*. While it looks like color.js has been updated to a working version, faker.js still appears to be affected, but the issue can be worked around by downgrading to a previous version (5.5.3).

The sabotaged versions cause applications to infinitely output strange letters and symbols

Bleeping Computer found that the developer of these two libraries, Marak Squires, introduced a malignant commit (a file revision on GitHub) to colors.js that adds “a new American flag module,” as well as rolled out version 6.6.6 of faker.js, triggering the same destructive turn of events. The sabotaged versions cause applications to infinitely output strange letters and symbols, beginning with three lines of text that read “LIBERTY LIBERTY LIBERTY.”

Even more curiously, the faker.js Readme file has also been changed to “What really happened with Aaron Swartz?” Swartz was a prominent developer who helped establish Creative Commons, RSS, and Reddit. In 2011, Swartz was charged for stealing documents from the academic database JSTOR with the purpose of making them free to access, and later committed suicide in 2013. Squires’ mention of Swartz could potentially

refer to conspiracy theories surrounding his death.

As pointed out by *Bleeping Computer*, a number of users – including some working with Amazon’s Cloud Development Kit – turned to GitHub’s bug tracking system to voice their concerns about the issue. And since `faker.js` sees nearly 2.5 million weekly downloads on npm, and `color.js` gets about 22.4 million downloads per week, the effects of the corruption are likely far-reaching. For context, `faker.js` generates fake data for demos, `color.js` adds colors to javascript consoles.

In response to the problem, Squires posted an update on GitHub to address the “zalgo issue,” which refers to the glitchy text that the corrupt files produce. “It’s come to our attention that there is a zalgo bug in the v1.4.44-liberty-2 release of colors,” Squires writes in a presumably sarcastic way. “Please know we are working right now to fix the situation and will have a resolution shortly.”

Two days after pushing the corrupt update to `faker.js`, Squires later sent out a tweet noting he’s been suspended from GitHub, despite storing hundreds of projects on the site. Judging by the changelog on both `faker.js` and `colors.js`, however, it looks like his suspension has already been lifted. Squires introduced the `faker.js` commit on January 4th, got banned on January 6th, and didn’t introduce the “liberty” version of `colors.js` until January 7th. It’s unclear whether Squires’ account has been banned again. *The Verge* reached out to GitHub with a request for comment but didn’t immediately hear back.

The story doesn’t end there, though. *Bleeping Computer* dug up one of Squires’ posts on GitHub from November 2020, in which he declares he no longer wants to do free work. “Respectfully, I am no longer going to support Fortune 500s (and other smaller sized companies) with my free work,” he says. “Take this as an opportunity to send me a six figure yearly contract or fork the project and have someone else work on it.”

Squires' bold move draws attention to the moral – and financial – dilemma of open-source development, which was likely the goal of his actions. A massive number of websites, software, and apps rely on open-source developers to create essential tools and components – all for free. It's the same issue that results in unpaid developers working tirelessly to fix the security issues in their open-source software, like the Heartbleed scare in 2014 that affected OpenSSL and the more recent Log4Shell vulnerability found in log4j that left volunteers scrambling to fix.

<https://www.theverge.com/2022/1/9/22874949/developer-corrupts-open-source-libraries-projects-affected>