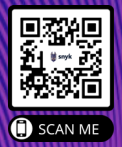
Are We Forever Doomed By Software Supply Chain Risks?

Steve Kinman

Field CISO, Snyk



snyk

- You care about software
- You care about software security
- You care about open -source software security

img-source: FORM&FICTION studio


UPLOAD

snyk

snyk

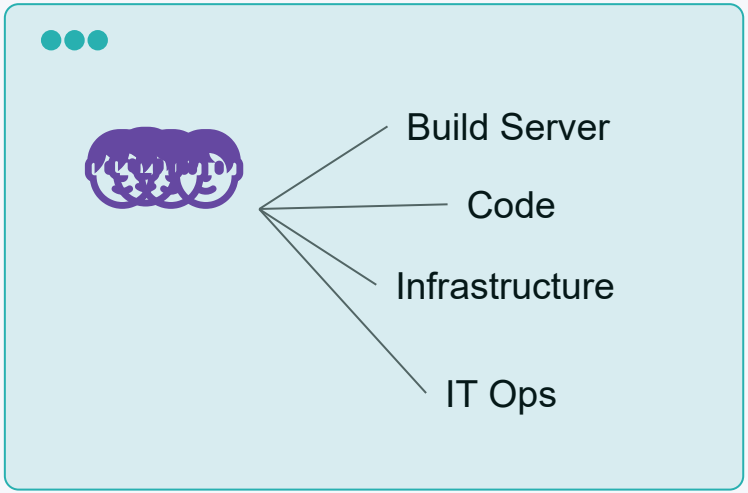
- What does the software supply chain landscape looks like today
- How developers play a role in security incidents
- Who do you trust?

“Software is eating the world”

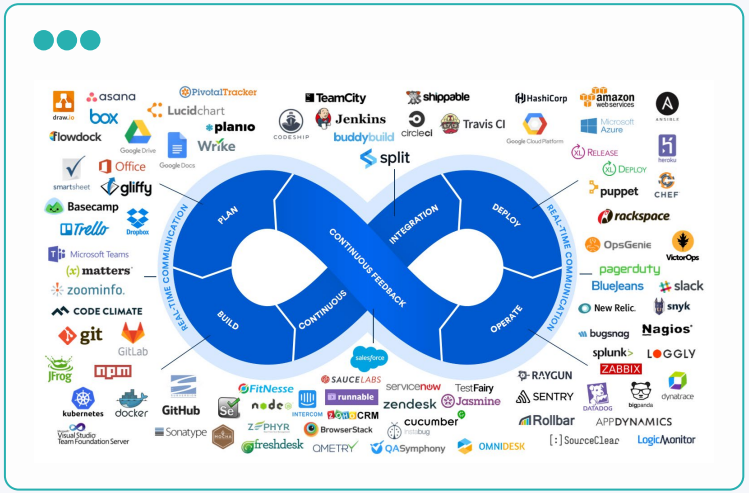
Applications are now CRITICAL components across all parts of modern life and business

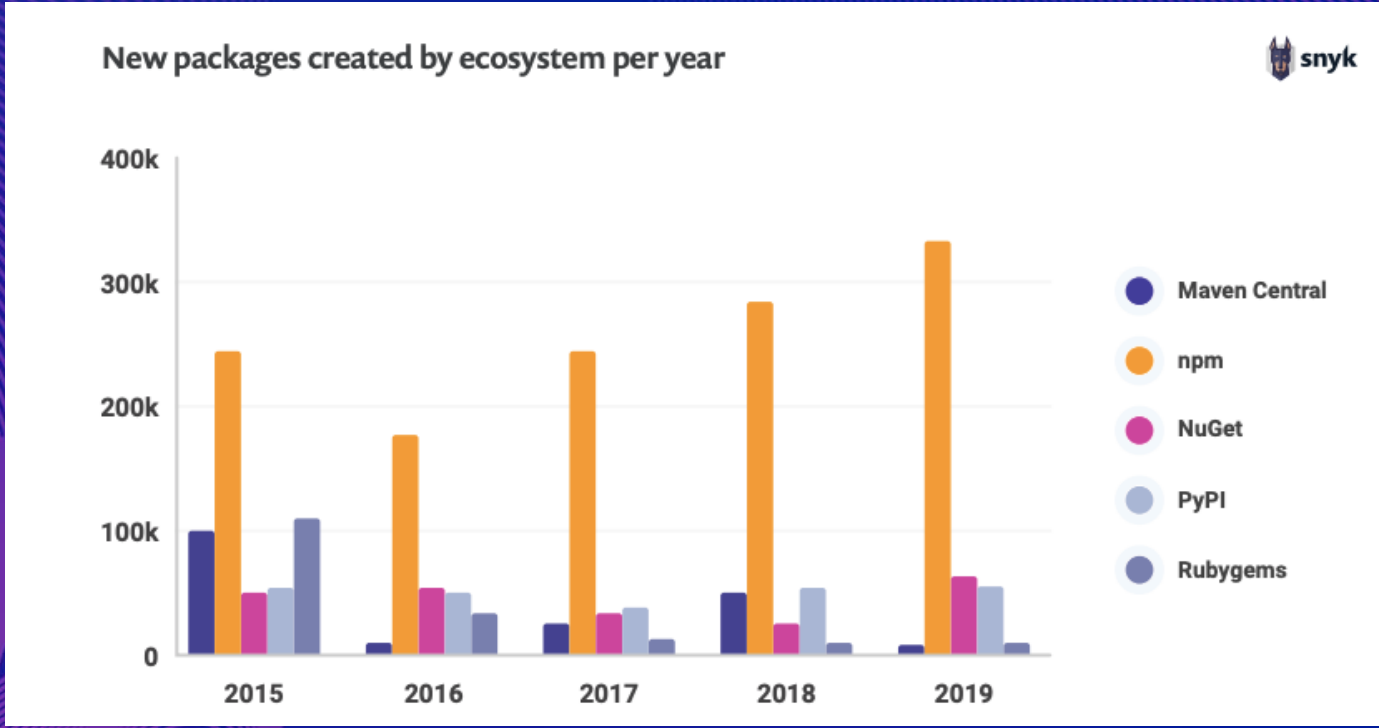
Success of digital revolution lead to the demand for rapid application creation

Before



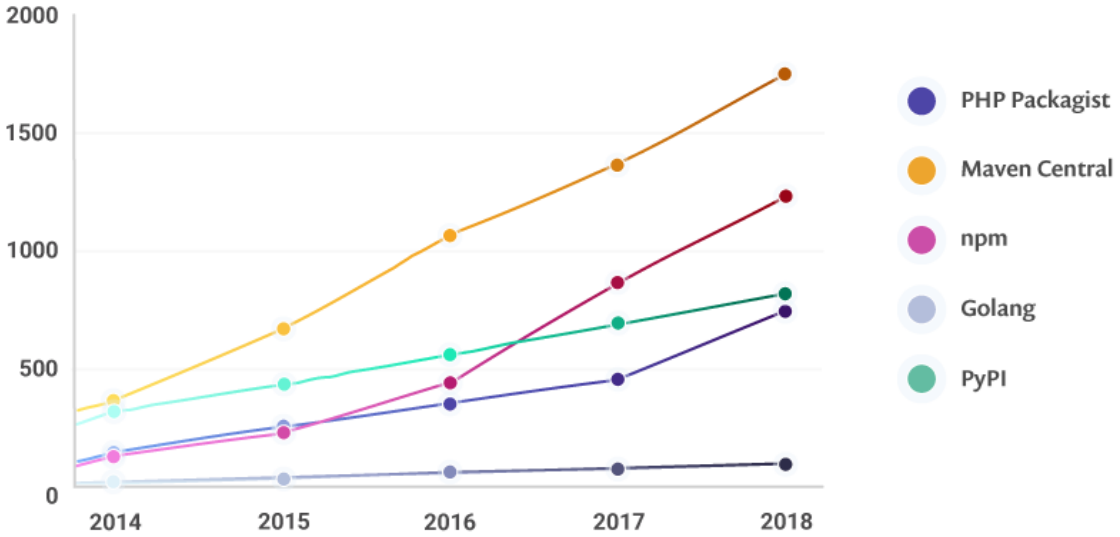
Now




New packages created by ecosystem per year
snyk
400k
300k
200k
100k
0
2015
2016
2017
2018
2019
Maven Central
npm
NuGet
PyPI
Rubygems

snyk

New vulnerabilities each year by ecosystem

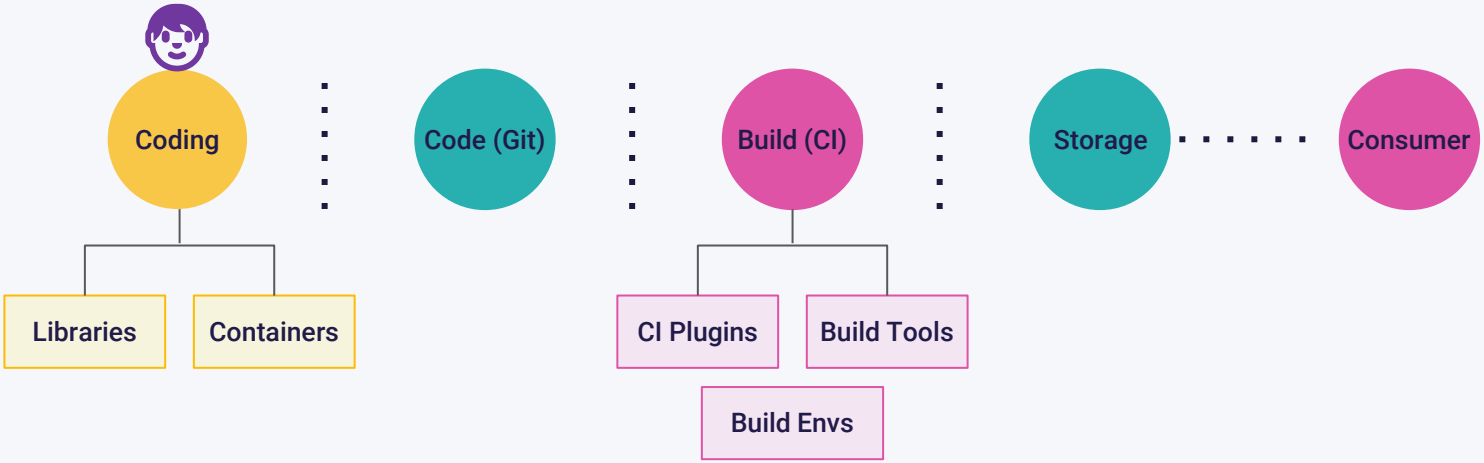


Software Supply Chain - Let's define it

What is the software supply chain?

The set of materials, tools, platforms and people involved in the creation of software products - the "software factory".

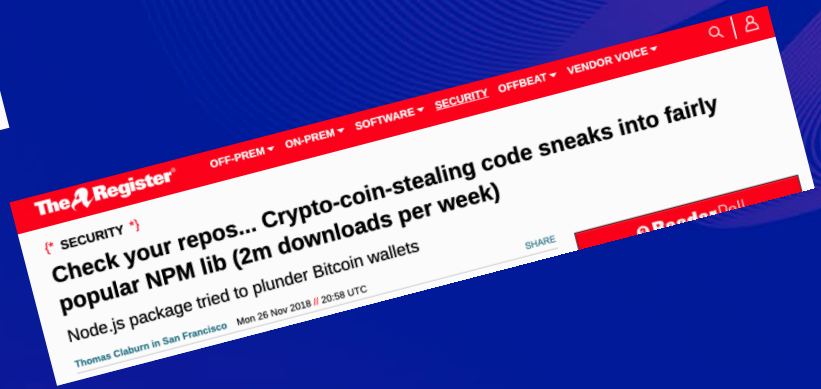
Like modern software, it is ever more distributed, open - source dependent and constantly - changing.



Developers as a Malware Distribution Vehicle

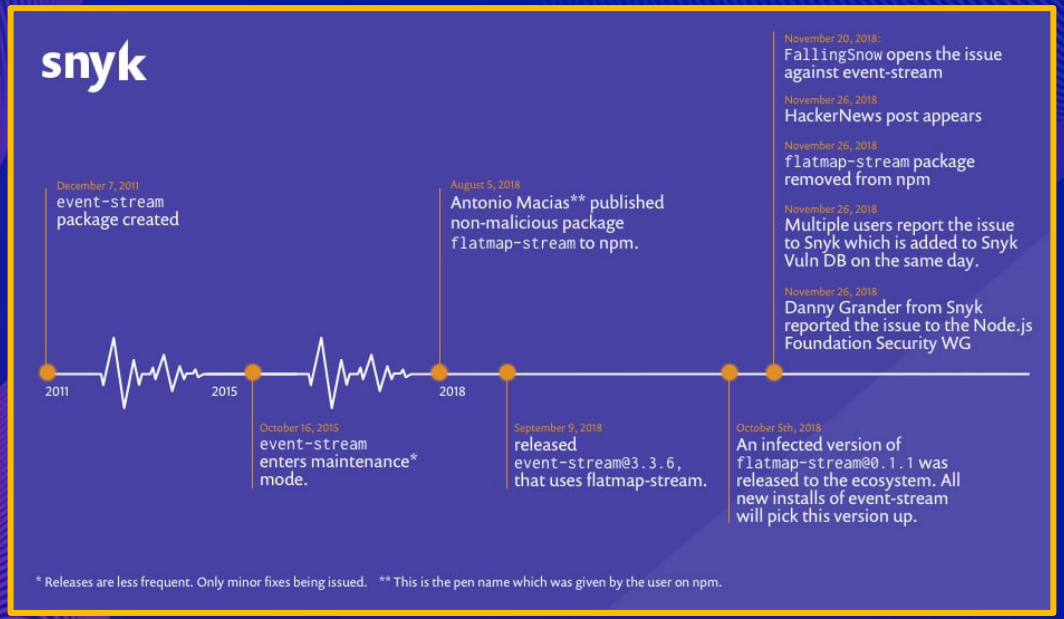
The event -stream incident

// 2018



snyk

The event -stream incident



source: http://bit.ly/es -incident

snyk

electron -native -notify
The ~~event-stream~~ incident

// 2019

- electron -native -notify@1.1.5 is not malicious
- user `sawlysawly` adds it to EASYDEX-GUI
- electron -native -notify@1.1.6 is malicious
- Agama Wallet rebuilt with most recent version

snyk

Attacking the heart of developer tooling

// 2021

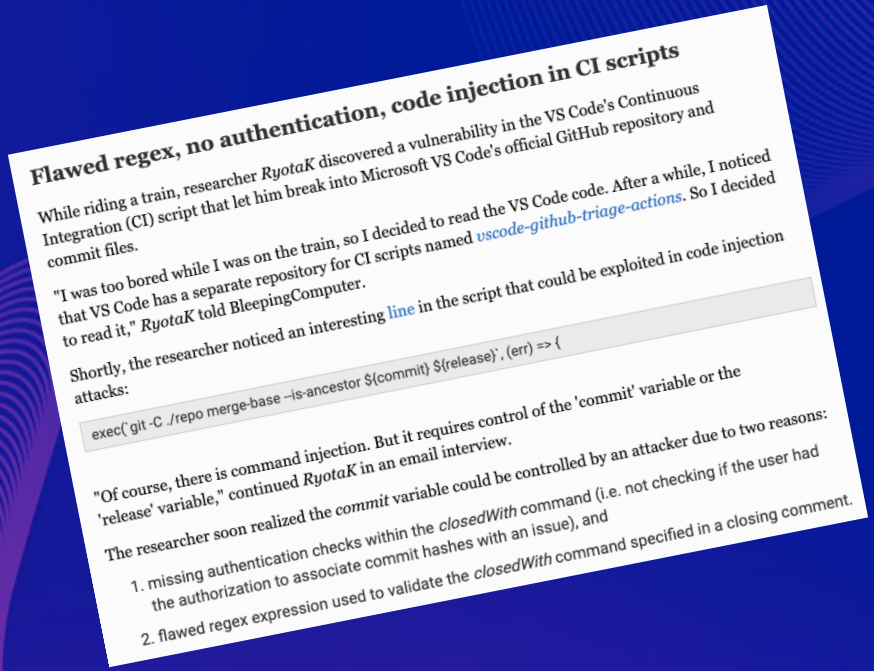
Attacking the heart of developer tooling

// 2021

snyk

Attacking the heart of developer tooling

// 2021



Flawed regex, no authentication, code injection in CI scripts

While riding a train, researcher *RyotaK* discovered a vulnerability in the VS Code's Continuous Integration (CI) script that let him break into Microsoft VS Code's official GitHub repository and commit files.

"I was too bored while I was on the train, so I decided to read the VS Code code. After a while, I noticed that VS Code has a separate repository for CI scripts named *vscode-github-triage-actions*. So I decided to read it," *RyotaK* told BleepingComputer.

Shortly, the researcher noticed an interesting line in the script that could be exploited in code injection attacks:

```
exec(`git -C ./repo merge-base --is-ancestor ${commit} ${release}`, (err) => {
```

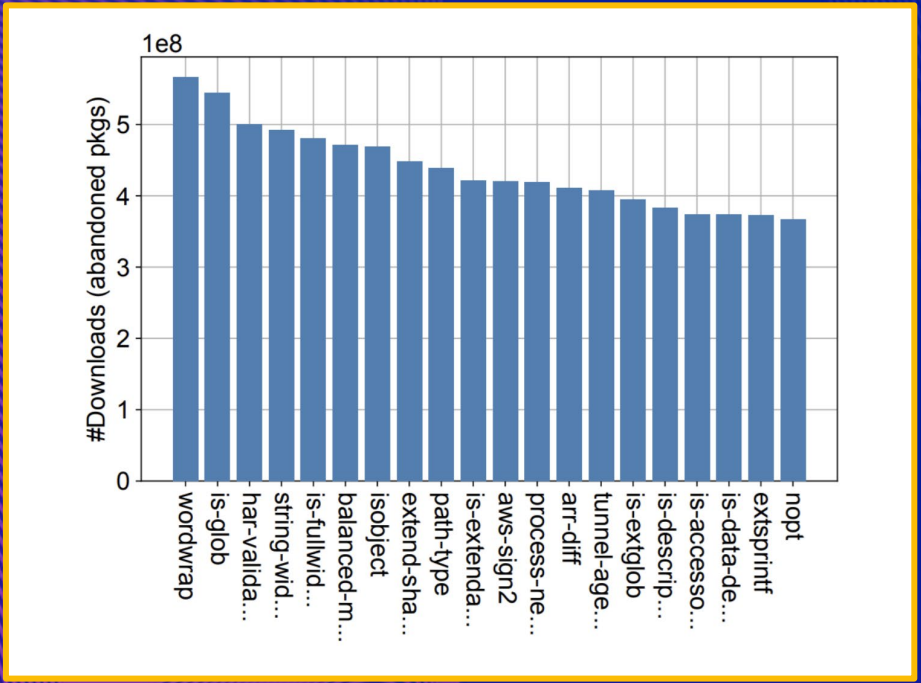
"Of course, there is command injection. But it requires control of the 'commit' variable or the 'release' variable," continued *RyotaK* in an email interview.

The researcher soon realized the *commit* variable could be controlled by an attacker due to two reasons:

1. missing authentication checks within the *closedWith* command (i.e. not checking if the user had the authorization to associate commit hashes with an issue), and
2. flawed regex expression used to validate the *closedWith* command specified in a closing comment.

snyk

The State of Open-Source Security



1,551,743 packages on npmjs

61% of open -source packages on npmjs are abandoned*

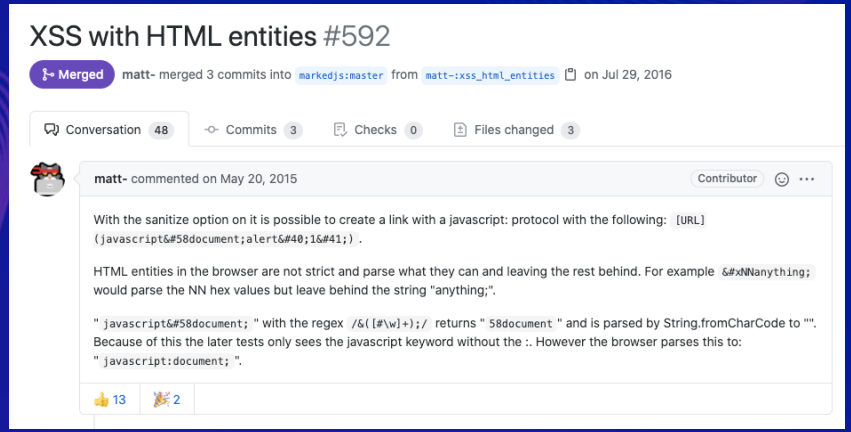
source: https://snyk.io/blog/how -much-do-we-really-know-about-how-packages-behave-on-the-npm-registry

snyk

The case of marked 's Cross-site Scripting vulnerability

// 2020

JavaScript Markdown parser,
millions of downloads

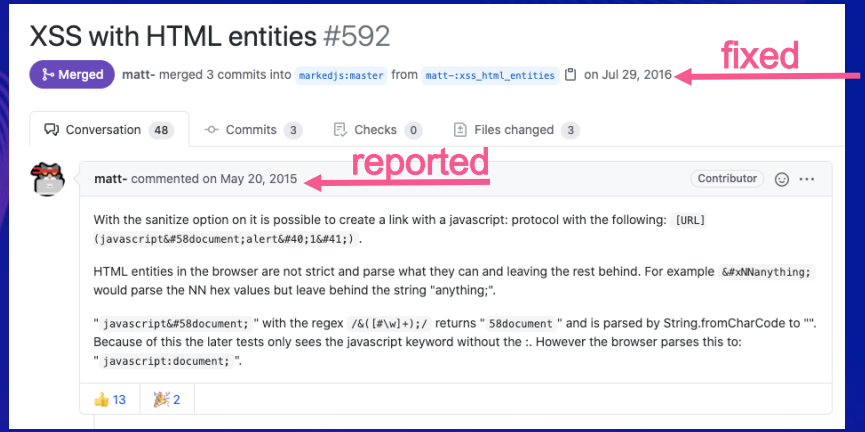


snyk

The case of marked 's Cross-site Scripting vulnerability

// 2020

JavaScript Markdown parser,
millions of downloads



snyk

Compromising Maintainer Accounts

Compromising Maintainer Accounts

// 2017

- 2017 research on weak npmjs credentials

Compromising Maintainer Accounts

// 2017

- 2017 research on weak npmjs credentials
- Publish access to 14% of npmjs ecosystem modules:
  `debug`, `ms`, `react`, `koa`, `request`, and more
- 4 accounts from top 20 downloaded modules
- 11% of users re-used their leaked password
  ‘Password’ used by a maintainer for millions of downloads

Can we do better for account security hygiene?

Can we do better for account security hygiene?

- npm, a registry of 1.5 million packages
- 2017: Supporting 2FA

Can we do better for account security hygiene?

- npm, a registry of 1.5 million packages
- 2017: Supporting 2FA
- 2019: 7.1% of npm package maintainers enabled 2FA

Can we do better for account security hygiene?

- npm, a registry of 1.5 million packages
- 2017: Supporting 2FA
- 2019: 7.1% of npm package maintainers enabled 2FA
- 2020: 9.27% of npm package maintainers enabled 2FA

snyk

“people often represent the weakest link in the security chain and are chronically responsible for the failure of security systems”

// Bruce Schneier, 2000

“given enough eyeballs, all bugs are shallow”

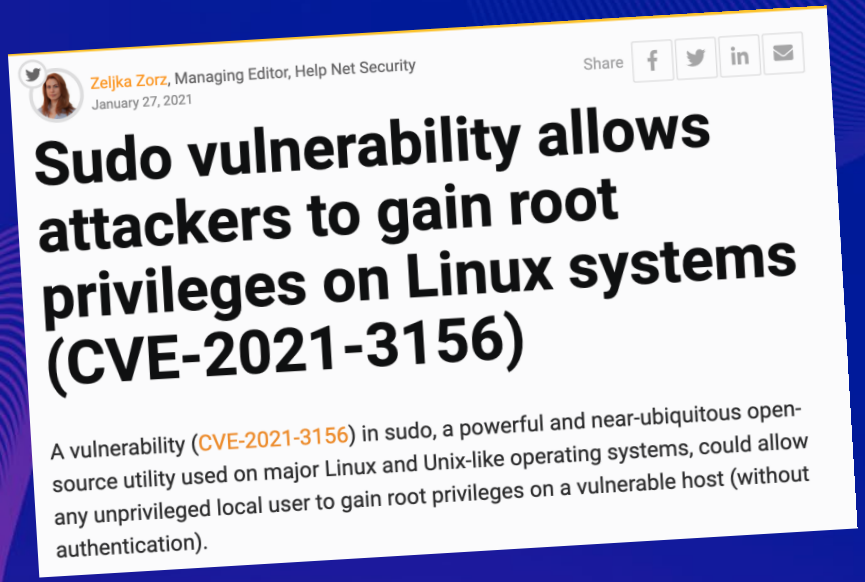
// The Cathedral and the Bazaar, 1999

“given enough eyeballs, all bugs are shallow”

// The Cathedral and the Bazaar, 1999

Oh really?

CVE-2021-3156: Heap-Based Buffer Overflow in Sudo



Zeljka Zorz, Managing Editor, Help Net Security
January 27, 2021

Share

Sudo vulnerability allows attackers to gain root privileges on Linux systems (CVE-2021-3156)

A vulnerability (CVE-2021-3156) in sudo, a powerful and near-ubiquitous open-source utility used on major Linux and Unix-like operating systems, could allow any unprivileged local user to gain root privileges on a vulnerable host (without authentication).

snyk

CVE-2021-3156:
Heap-Based Buffer Overflow in Sudo

“Any unprivileged user can gain root privileges on a vulnerable host using a default sudo configuration by exploiting this vulnerability.”

snyk

CVE-2021-3156:
Heap-Based Buffer Overflow in Sudo

"The vulnerability itself has been hiding in plain sight for nearly 10 years. It was introduced in July 2011 (commit 8255ed69) and affects all legacy versions from 1.8.2 to 1.8.31p2 and all stable versions from 1.9.0 to 1.9.5p1 in their default configuration."

snyk

Software Supply Chain risks
impact everyone

Diamonds are forever,

but what about your open -source libraries ?

What happens when maintainers remove their libraries ?

// 2016

The Register

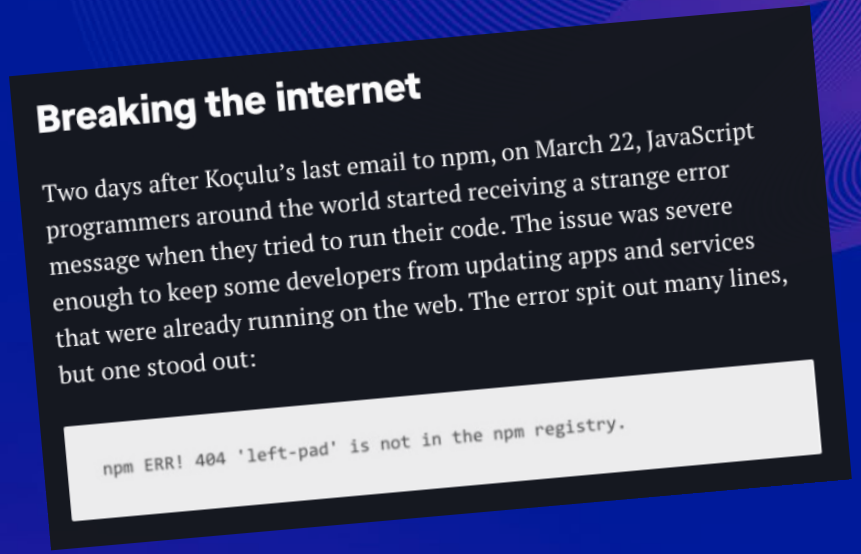
{* SOFTWARE *}

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

SHARE

Chris Williams, Editor in Chief Wed 23 Mar 2016 // 01:24 UTC



Breaking the internet

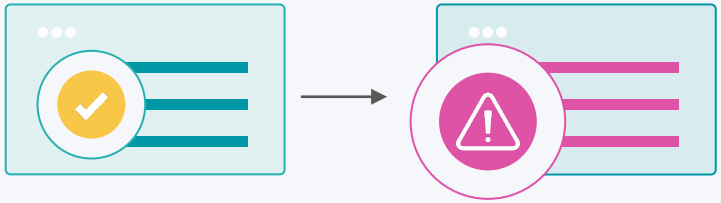
Two days after Koçulu's last email to npm, on March 22, JavaScript programmers around the world started receiving a strange error message when they tried to run their code. The issue was severe enough to keep some developers from updating apps and services that were already running on the web. The error spit out many lines, but one stood out:

```
npm ERR! 404 'left-pad' is not in the npm registry.
```


snyk

Software Supply Chain - Attacks

Exploit the weakest link



Attack once…..infiltrate many
(Cascading Attack)

Gartner predicts that by 2025, **45%** of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021

Are we going to have
less, or more software in the future?

Are we going to use
less, or more open-source software ?

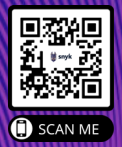
Who do you trust ?

img-source: FORM&FICTION studio

snyk

Who do you trust ?

Steve Kinman
Field CISO @Snyk



Get your Snyk shirt!

snyk