StrangerDanger!

Finding Security Vulnerabilities Before They Find You!

Liran Tal

snyk

@liran_tal

DevDays Europe, May 15th 2019

Liran Tal
Developer Advocate at Snyk

@liran_tal

Node.js Security WG

OWASP NodeGoat Team

Author of Essential Node.js Security

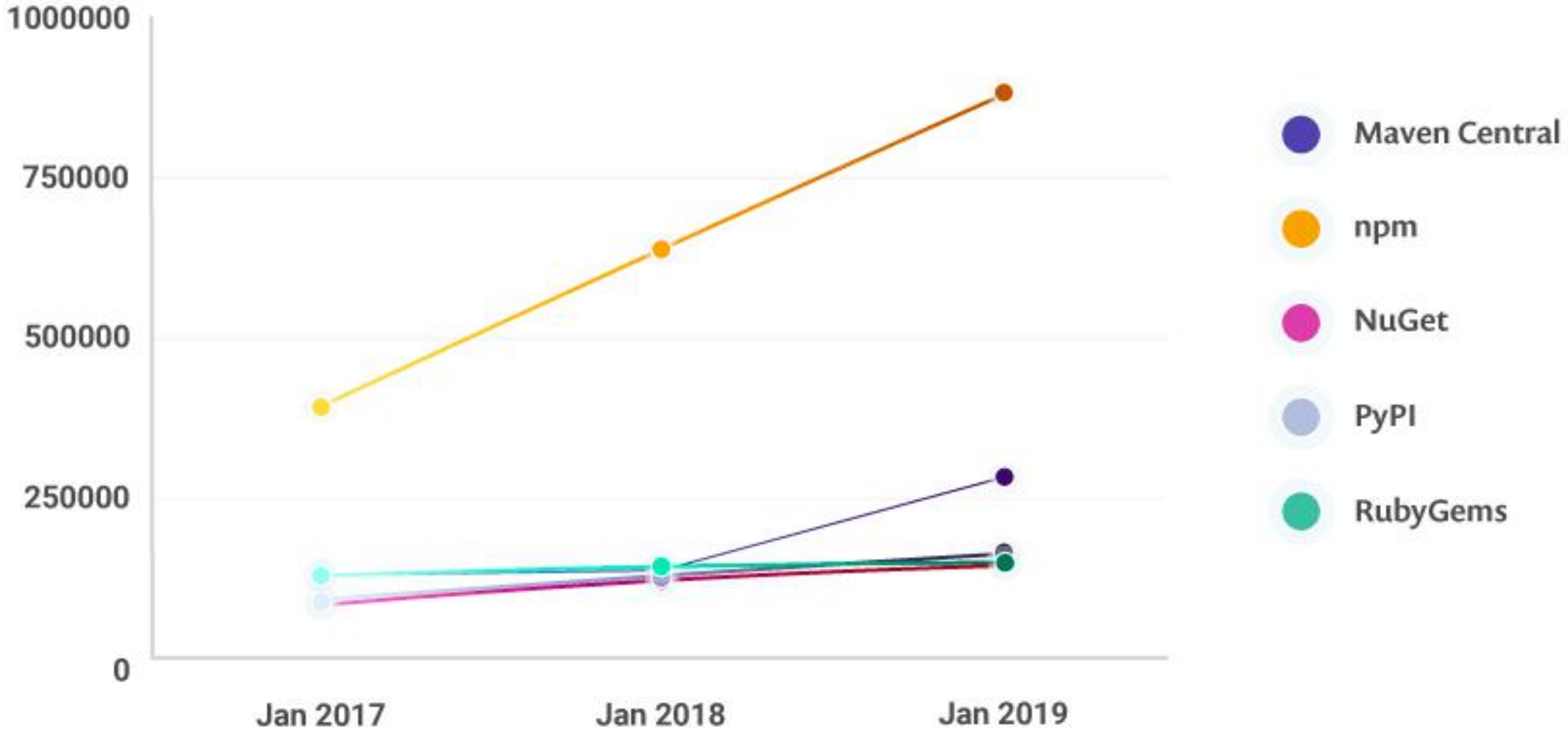
THE SECURE DEVELOPER

JSHeroes

Open Source Is Awesome

Total packages indexed per ecosystem

snyk

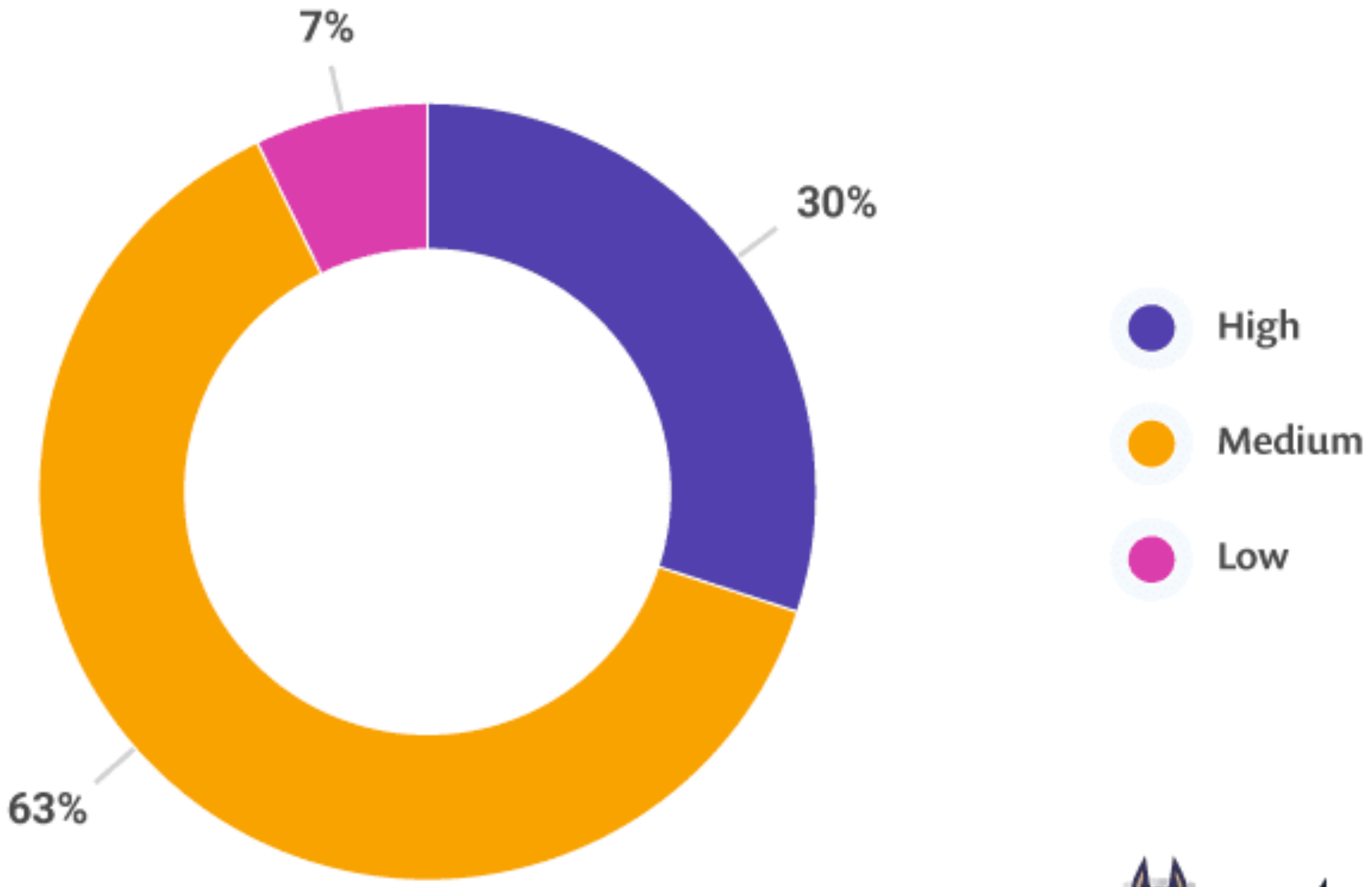


Open Source is written by People

Do You Know
Which Dependencies
You Have?

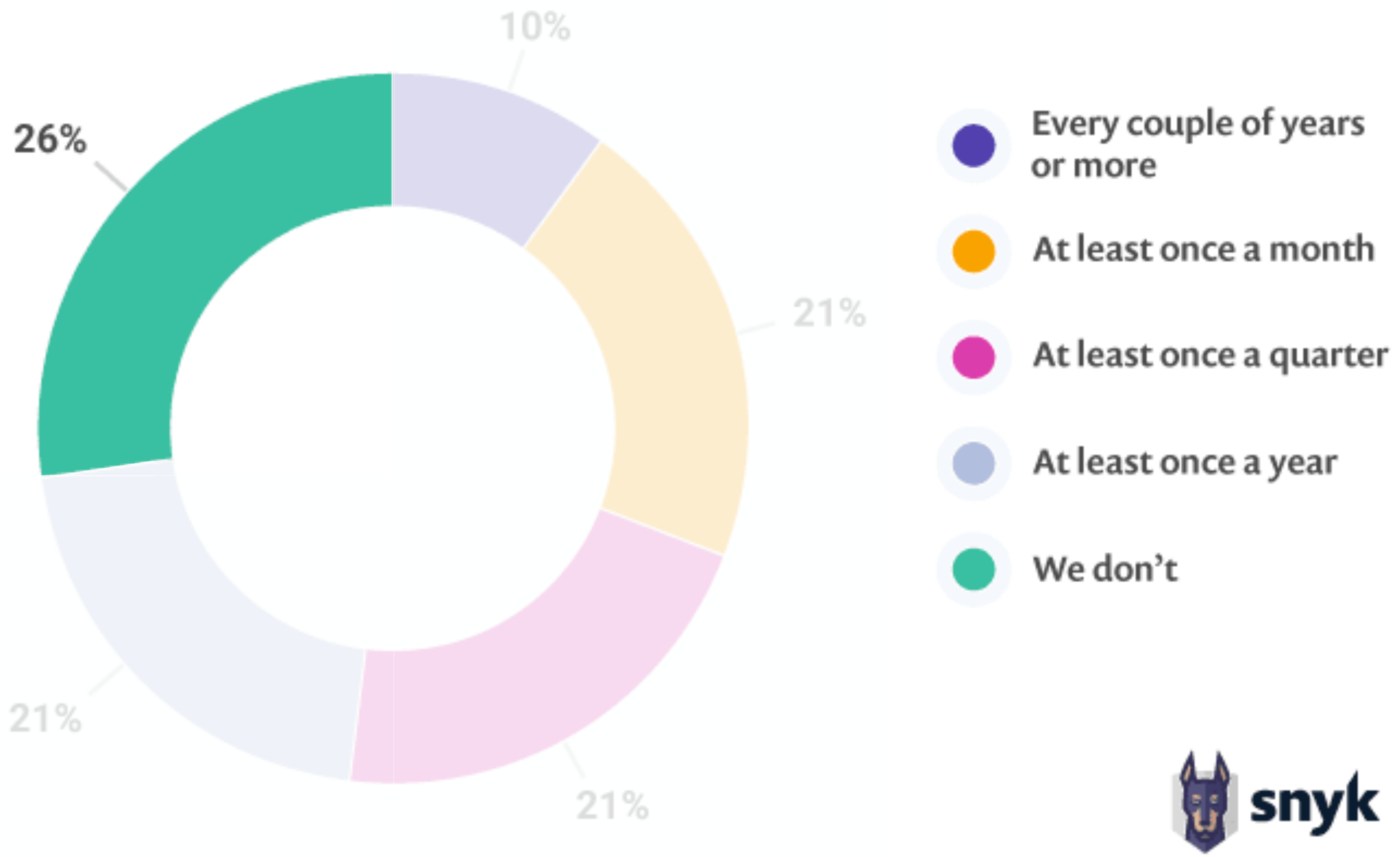
Open Source is written by ~~People~~ Strangers

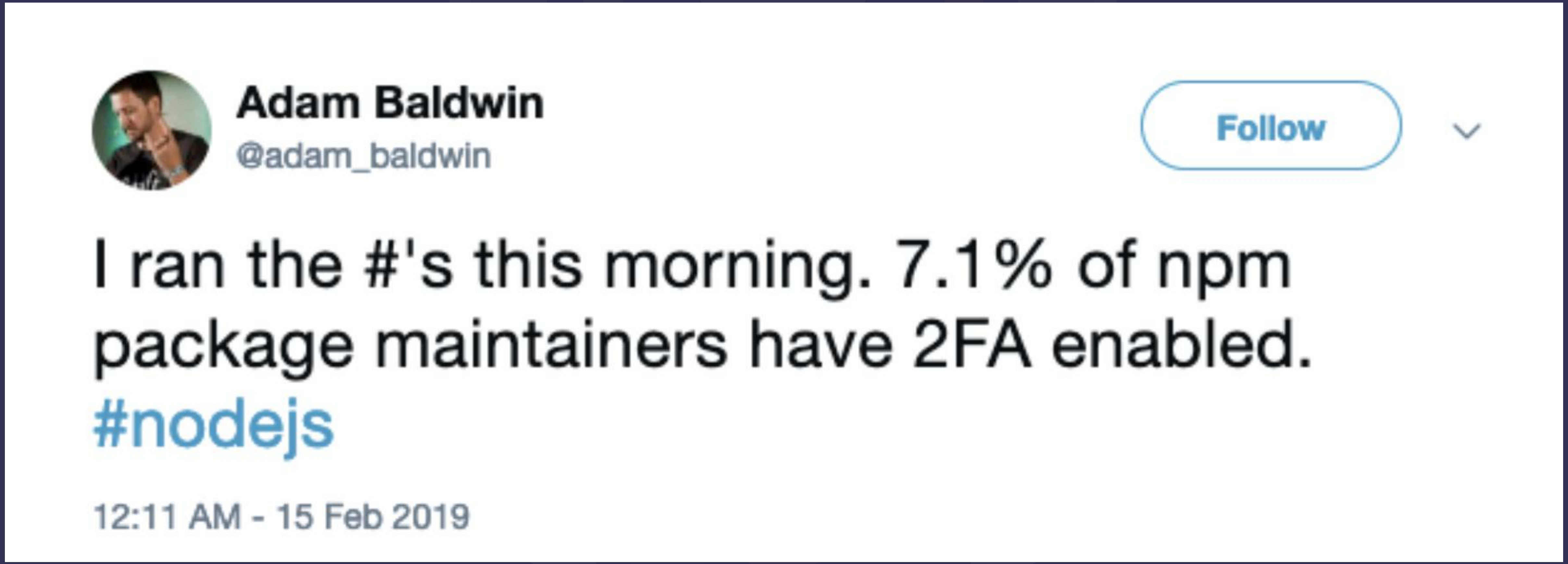
OS maintainers are confident in their own security knowledge



snyk

OS maintainers differ in their code auditing cadence





Adam Baldwin
@adam_baldwin

I ran the #'s this morning. 7.1% of npm package maintainers have 2FA enabled. #nodejs

12:11 AM - 15 Feb 2019

flatmap-stream

eslint-scope

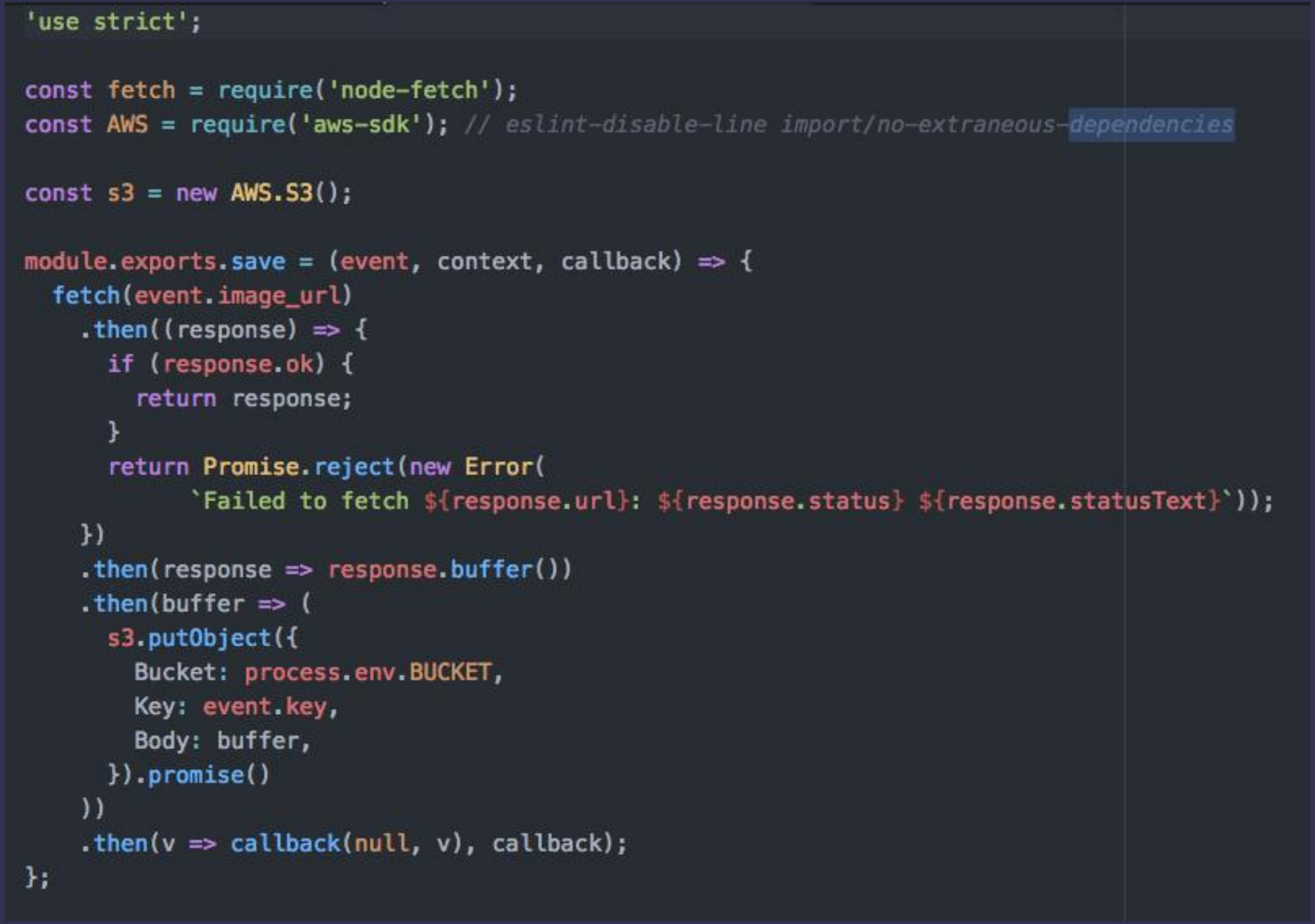
crossenv

A typical JavaScript app has 100s or 1,000s of dependencies

Some direct, most indirect

Serverless Example: Fetch file & store in s3

(Serverless Framework Example)



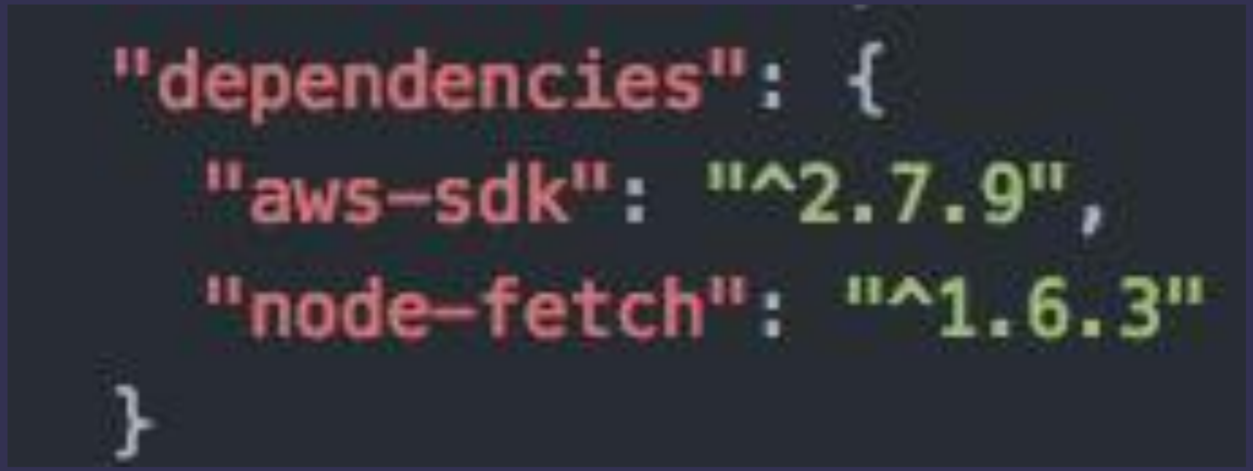
```
'use strict';

const fetch = require('node-fetch');
const AWS = require('aws-sdk'); // eslint-disable-line import/no-extraneous-dependencies

const s3 = new AWS.S3();

module.exports.save = (event, context, callback) => {
  fetch(event.image_url)
    .then((response) => {
      if (response.ok) {
        return response;
      }
      return Promise.reject(new Error(
            `Failed to fetch ${response.url}: ${response.status} ${response.statusText}`));
    })
    .then(response => response.buffer())
    .then(buffer => (
      s3.putObject({
        Bucket: process.env.BUCKET,
        Key: event.key,
        Body: buffer,
      }).promise()
    ))
    .then(v => callback(null, v), callback);
};
```

19 Lines of Code

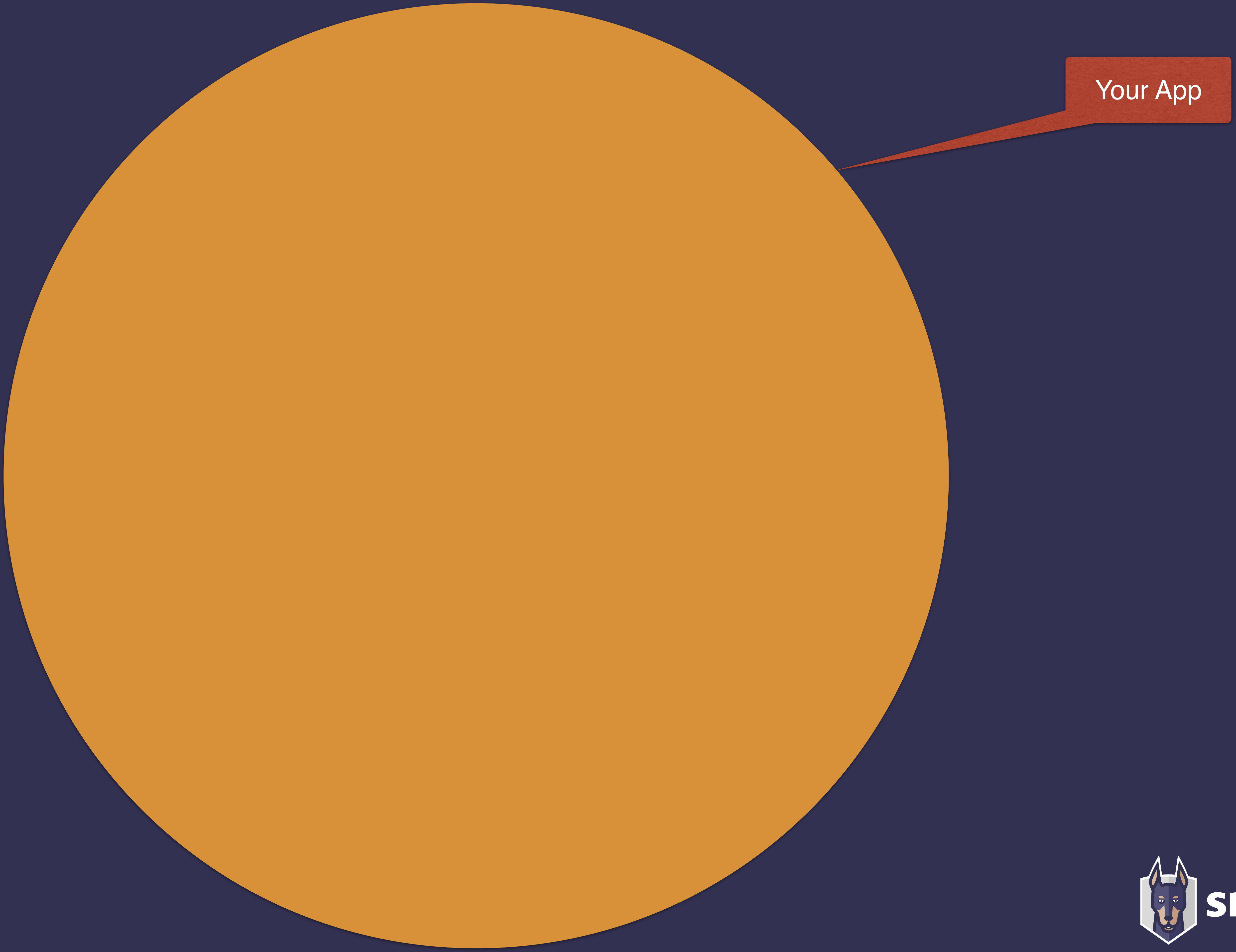


```
"dependencies": {
  "aws-sdk": "^2.7.9",
  "node-fetch": "^1.6.3"
}
```

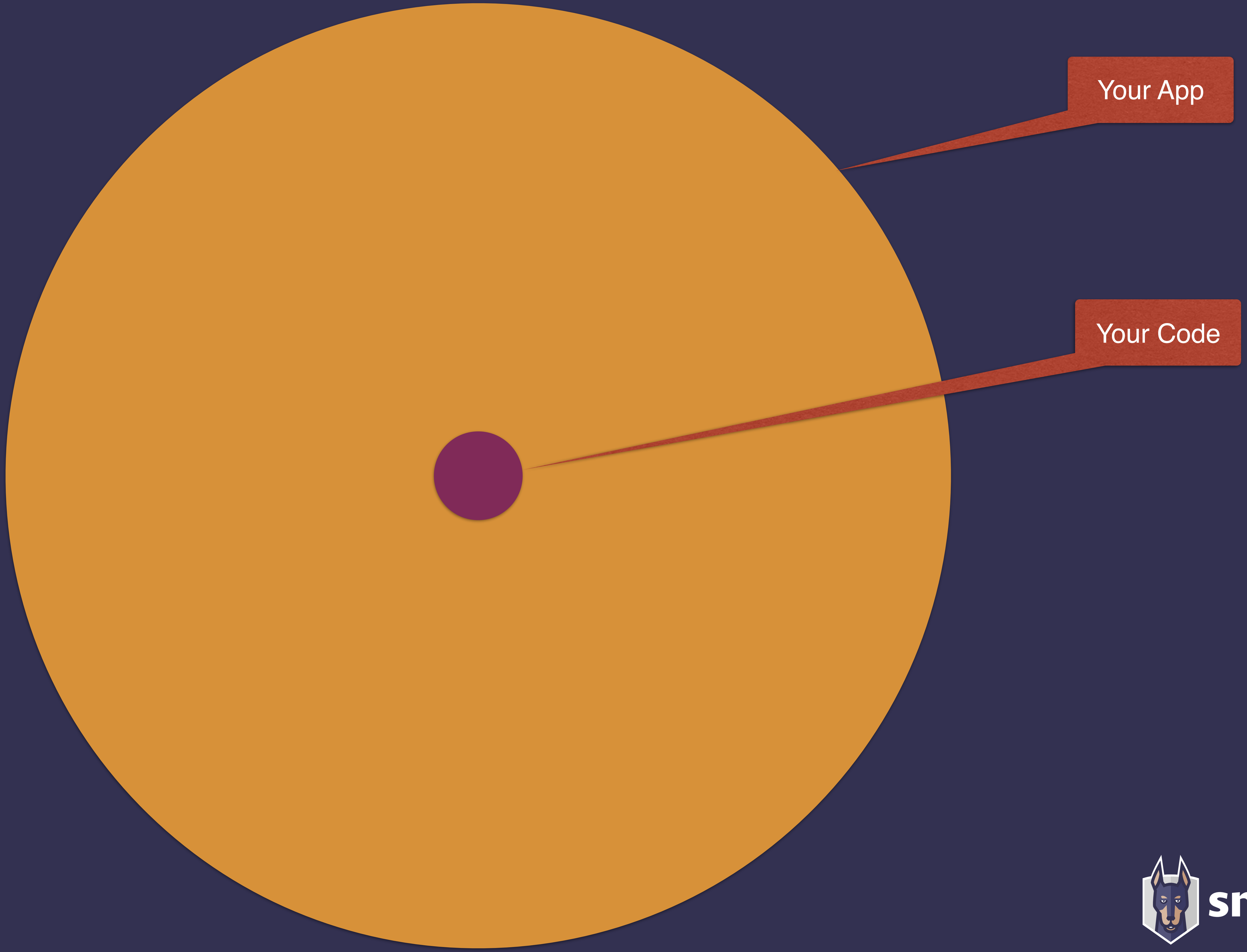
2 Direct dependencies

19 dependencies (incl. indirect)

191,155 Lines of Code



Your App



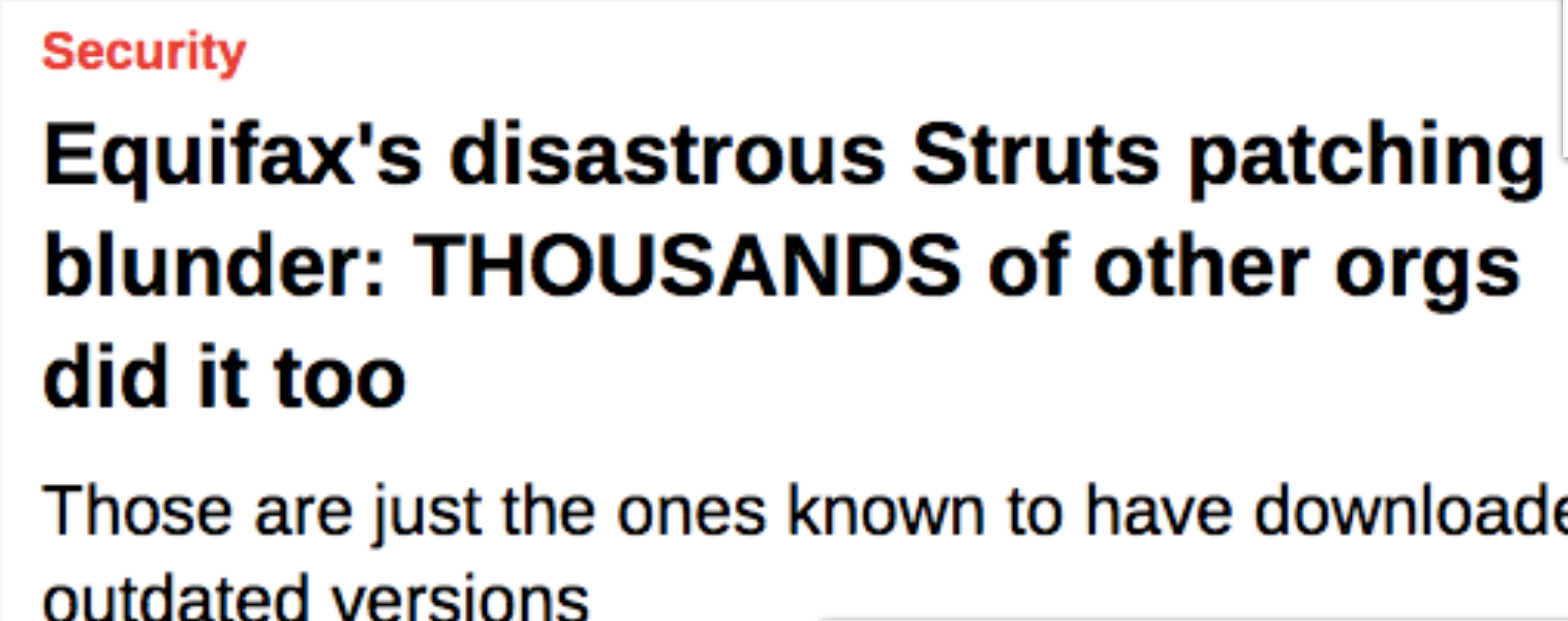
Your App

Your Code

AppSec Challenges

1. Software delivery **sped up** with little thought to **security**
2. **Lack of security focus** throughout the app lifecycle
3. **Silo**-ed security expertise

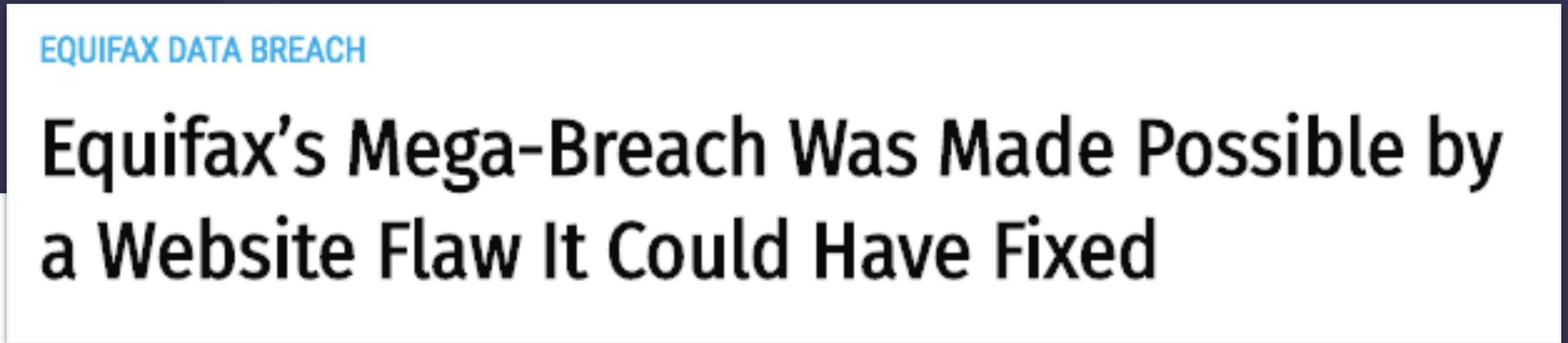
What happens when we neglect open source security?



Security

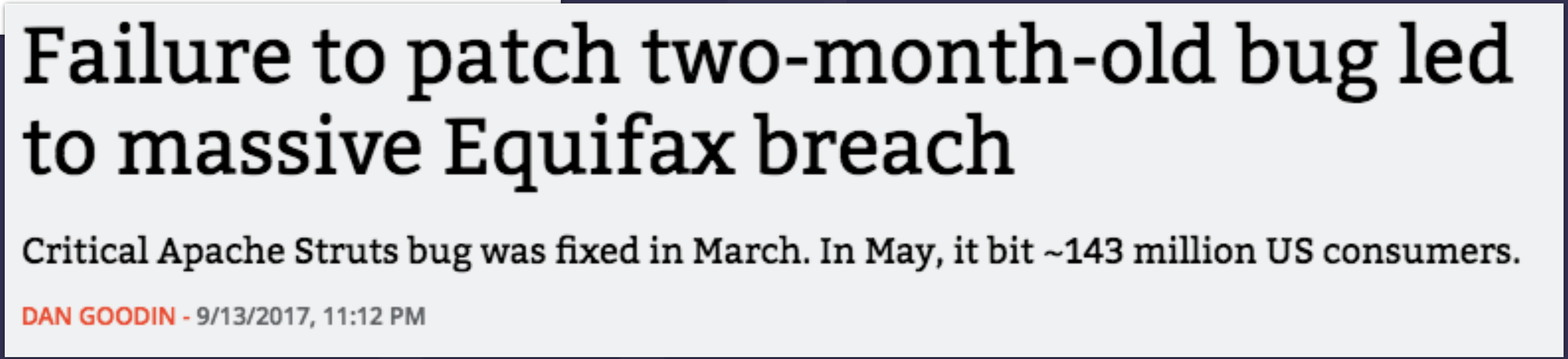
Equifax's disastrous Struts patching blunder: THOUSANDS of other orgs did it too

Those are just the ones known to have downloaded outdated versions



EQUIFAX DATA BREACH

Equifax's Mega-Breach Was Made Possible by a Website Flaw It Could Have Fixed



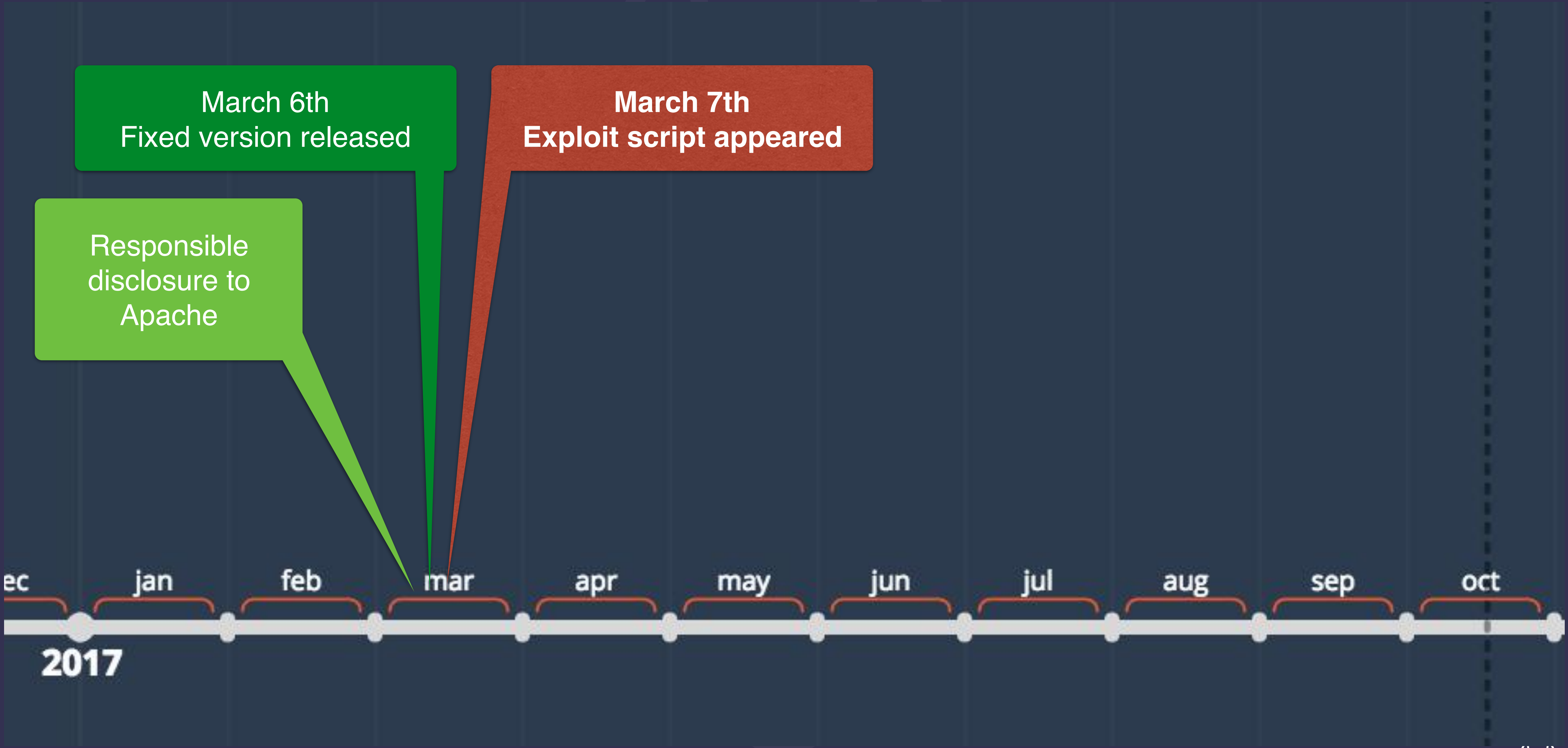
Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

DAN GOODIN - 9/13/2017, 11:12 PM

Java Struts 2 RCE Vulnerability

CVE 2017-5638



March 6th
Fixed version released

March 7th
Exploit script appeared

Responsible disclosure to Apache

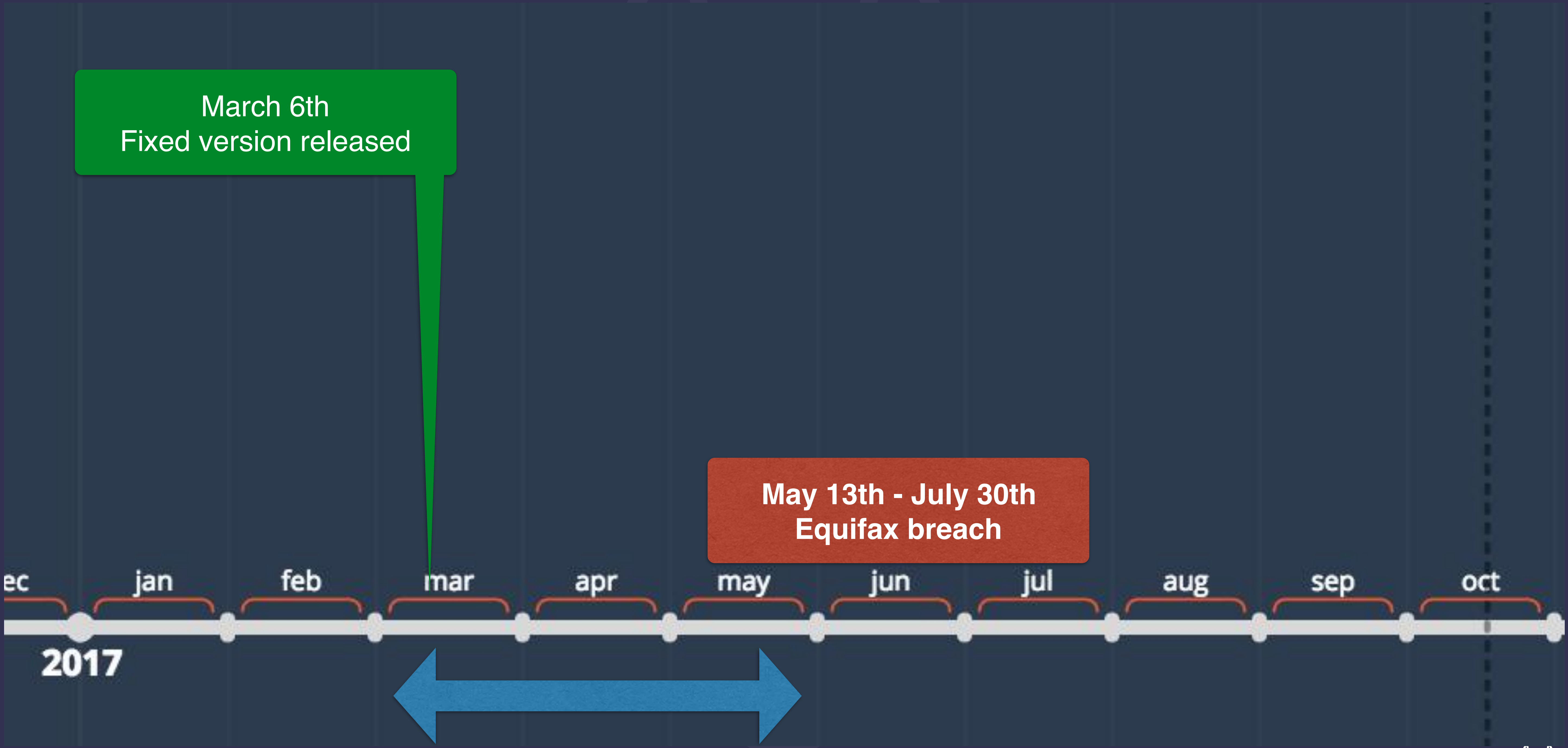
@liran_tal

Source: Josh Corman & Dan Geer

snyk

Java Struts 2 RCE Vulnerability

CVE 2017-5638



March 6th
Fixed version released

May 13th - July 30th
Equifax breach

@liran_tal

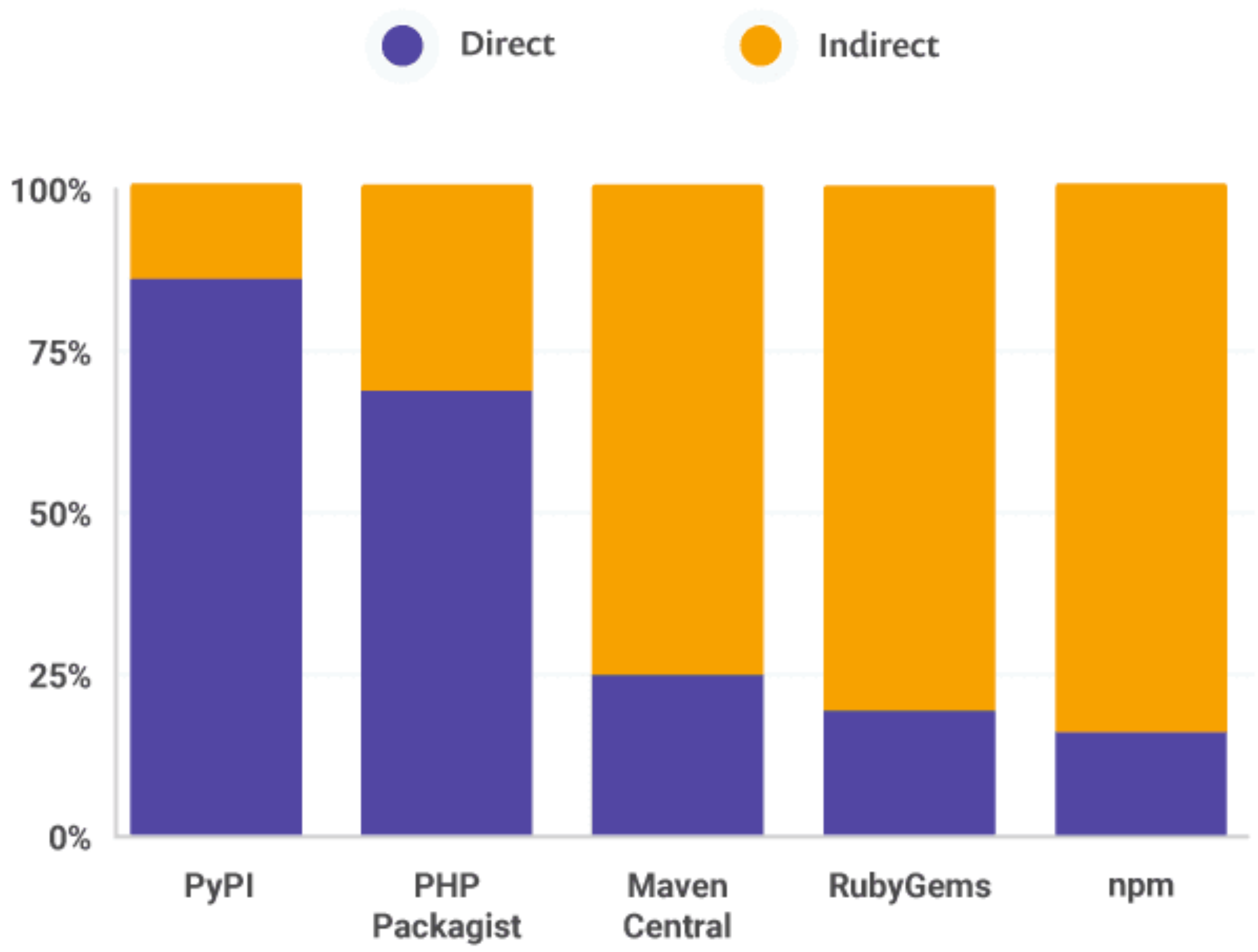
Source: Josh Corman & Dan Geer

snyk

Attackers Are Targeting Open Source

One vulnerability, many victims

The direct and indirect dependency split across ecosystems



Live Hacking

Let’s learn about vulnerabilities in open source libraries

What’s the **Solution**?

What’s the **Solution?**

Team Culture + Process + Tooling

Open Source Security Takeaway

- Find vulnerabilities
- Fix vulnerabilities
  - Upgrade when possible, patch when needed
- Prevent adding vulnerable modules
  - Break the build, test in pull requests

Liran Tal
Developer Advocate

Open Source Is Awesome

Please Enjoy Responsibly

@liran_tal