Exploiting and Fixing Common Vulnerabilities in Your (Java) Web Application

Brian Vermeer
@BrianVerm

snyk.io

snyk

Stranger Danger

Brian Vermeer
@BrianVerm

snyk.io

snyk

ABOUT **ME**

BRIAN VERMEER
DEVELOPER ADVOCATE
@BRIANVERM
BRIANVERMEER@SNYK.IO

snyk.io

snyk

Oracle
Groundbreaker
Ambassador

snyk

DevSecOps

snyk.io

snyk

What are the **Problems?**

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

How **bad** is the **Situation?**

~59%
of Reported Vulnerabilities in Maven Central Packages
Remain Unfixed

Source: Josh Corman & Dan Geer

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Those are just the ones known to have downloaded outdated versions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

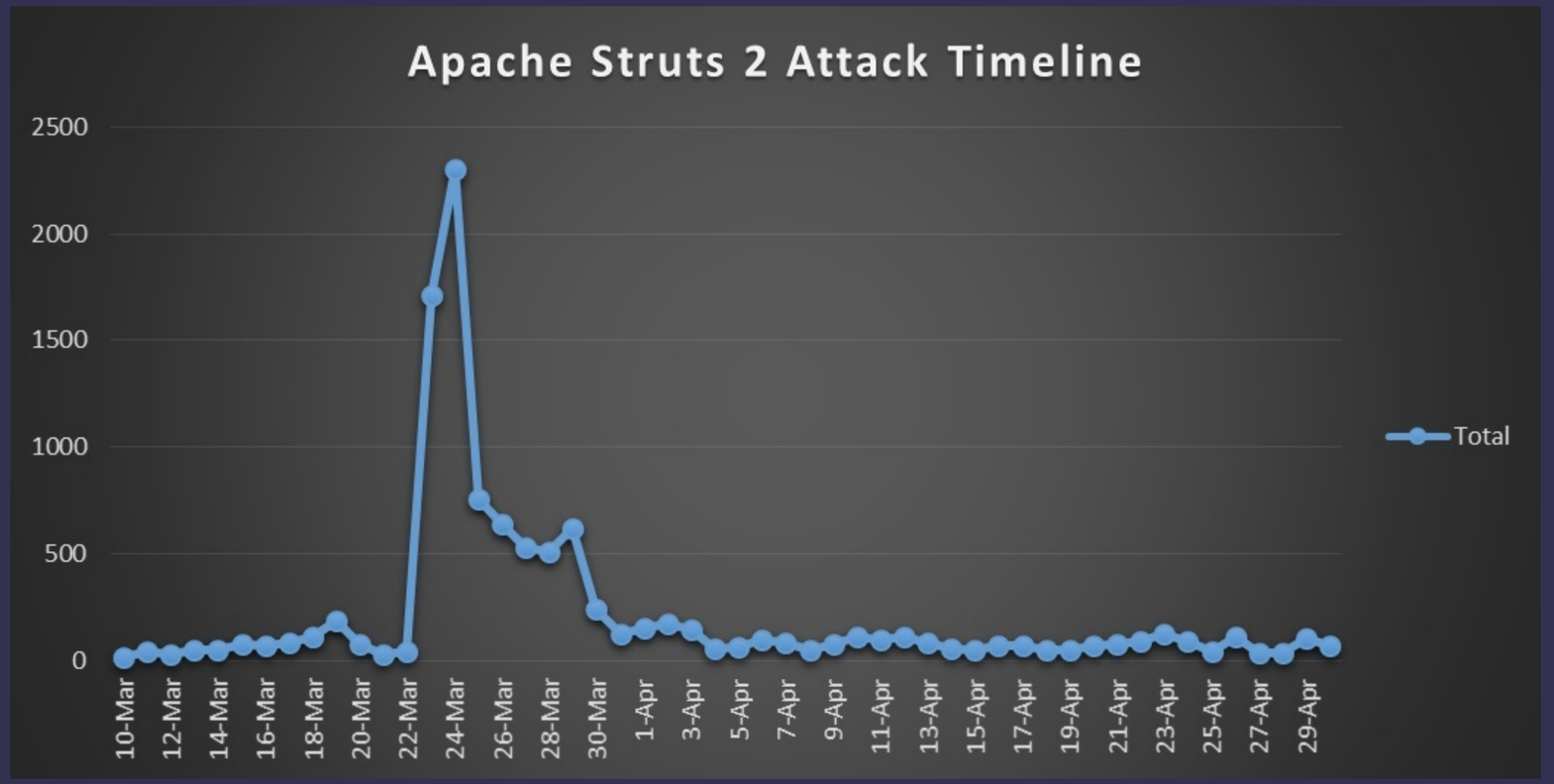
Failure to patch two-month-old bug led to massive Equifax breach

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



Source: SecurityIntelligence.com

Let’s pick on JavaScript

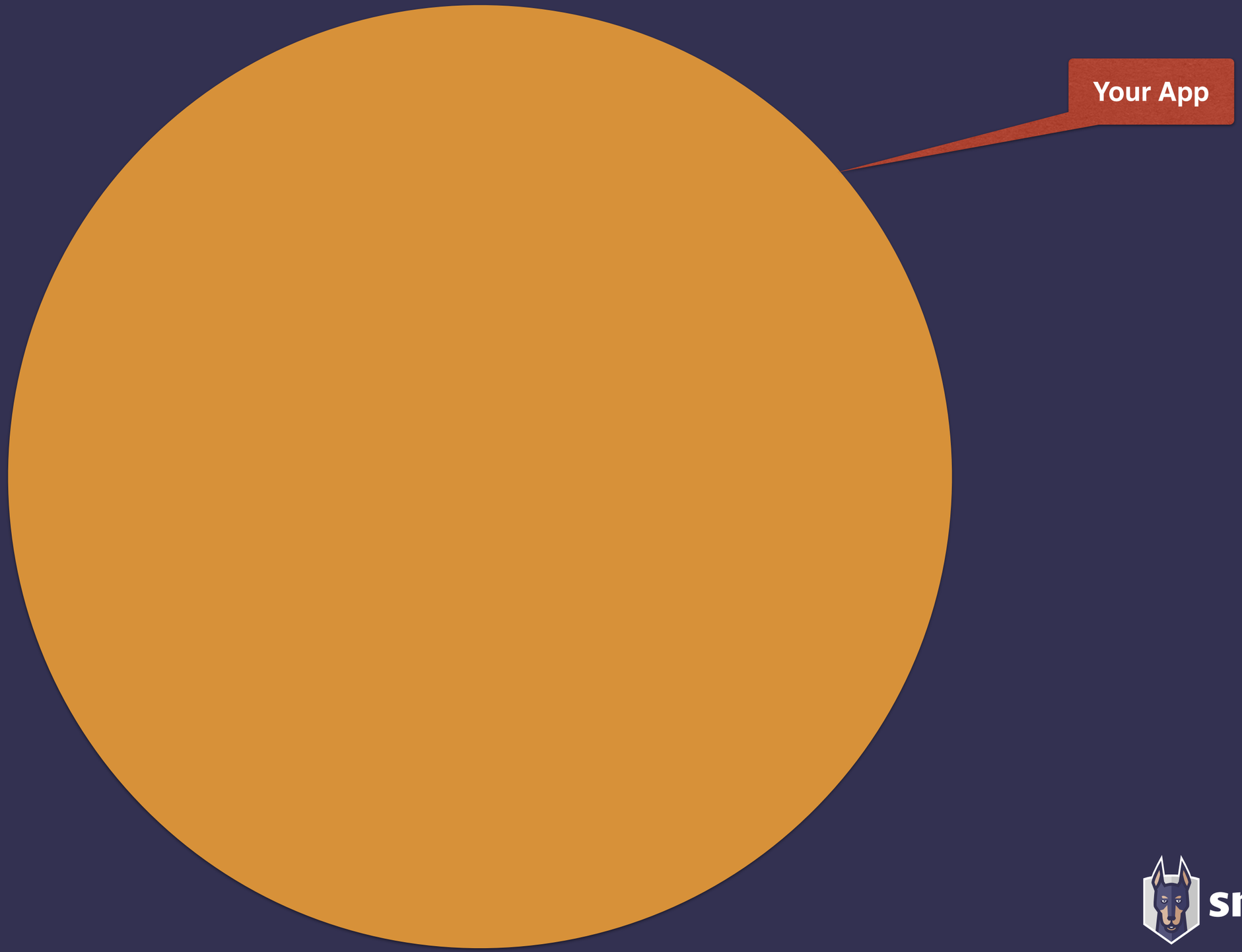
npm usage

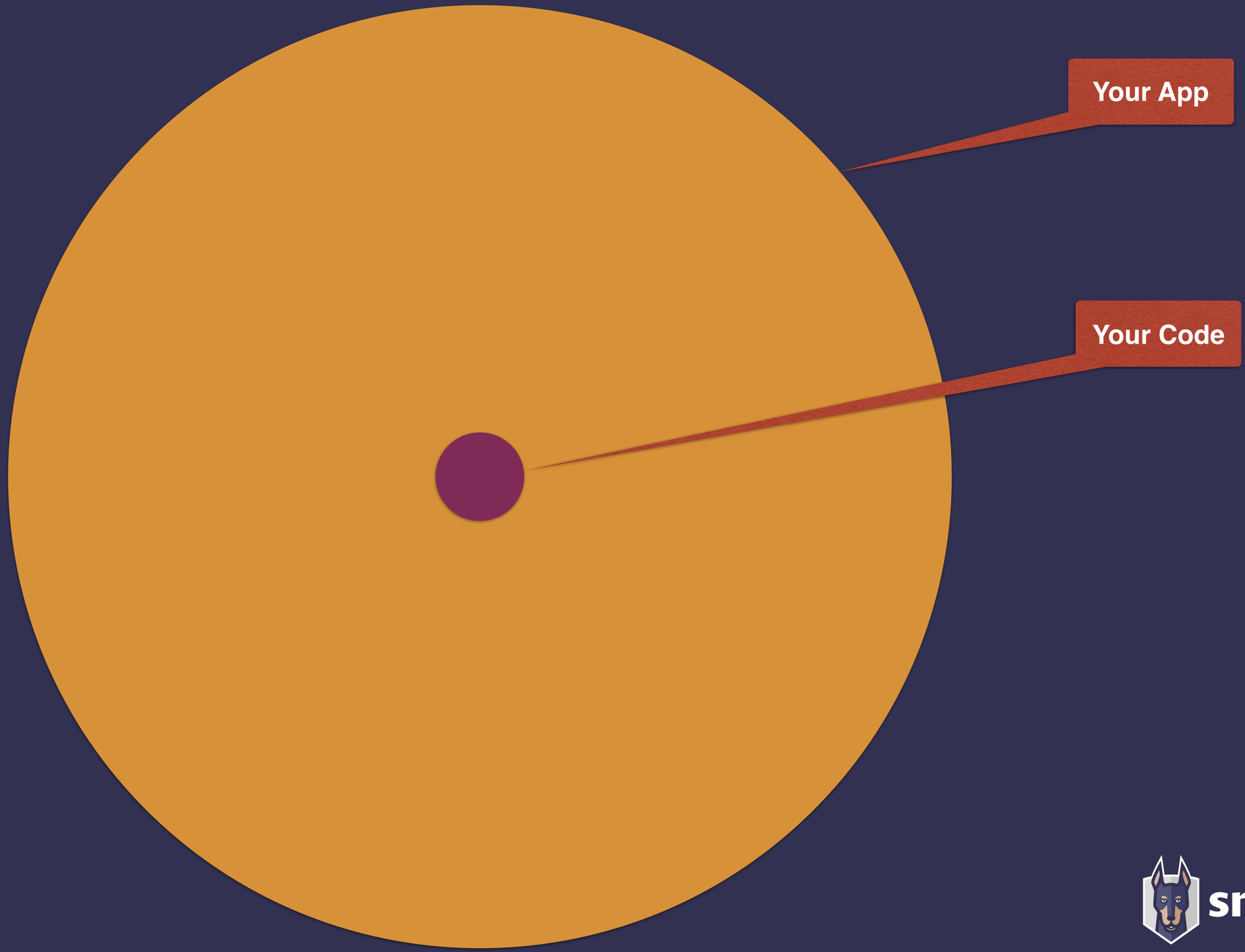
Has Exploded

>400,000 packages

>6B downloads/month

>70,000 publishers


Your App



snyk

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

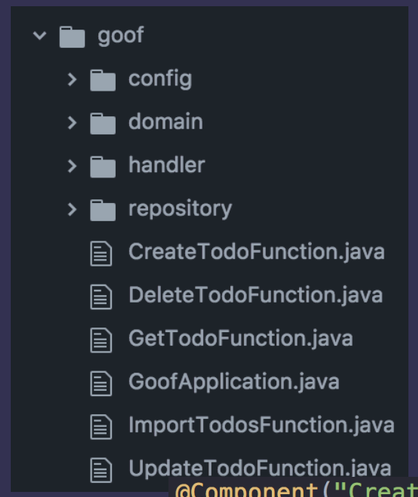
```
"dependencies": {
  "aws-sdk": "^2.7.9",
  "node-fetch": "^1.6.3"
}
```

2 Direct dependencies

19 dependencies (incl. indirect)

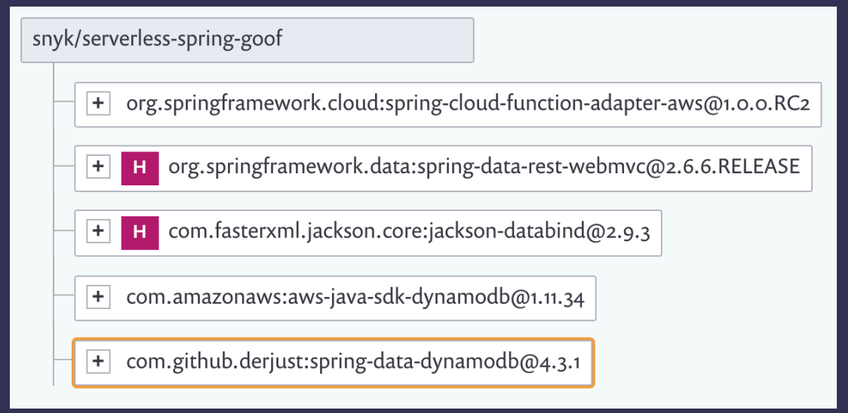
191,155 Lines of Code

Spring Serverless Example




```java
@Component("CreateTodoFunction")
public class CreateTodoFunction implements Function<TodoRequest, TodoResponse> {

  @Autowired
  TodoRepository repository;

  public Todo createTodo(final Todo todo) {
        return repository.save(todo);
    }

    @Override
    public TodoResponse apply(final TodoRequest todoRequest) {
        final TodoResponse result = new TodoResponse();

        result.setResult(createTodo(todoRequest.getTodo()));

        return result;
    }
}
```

222 Lines of Code



5 Direct dependencies

54 dependencies (incl. indirect)

460,046 Lines of Code

snyk.io

snyk

Open Source Usage Has Exploded

Attackers Are Targeting Open Source

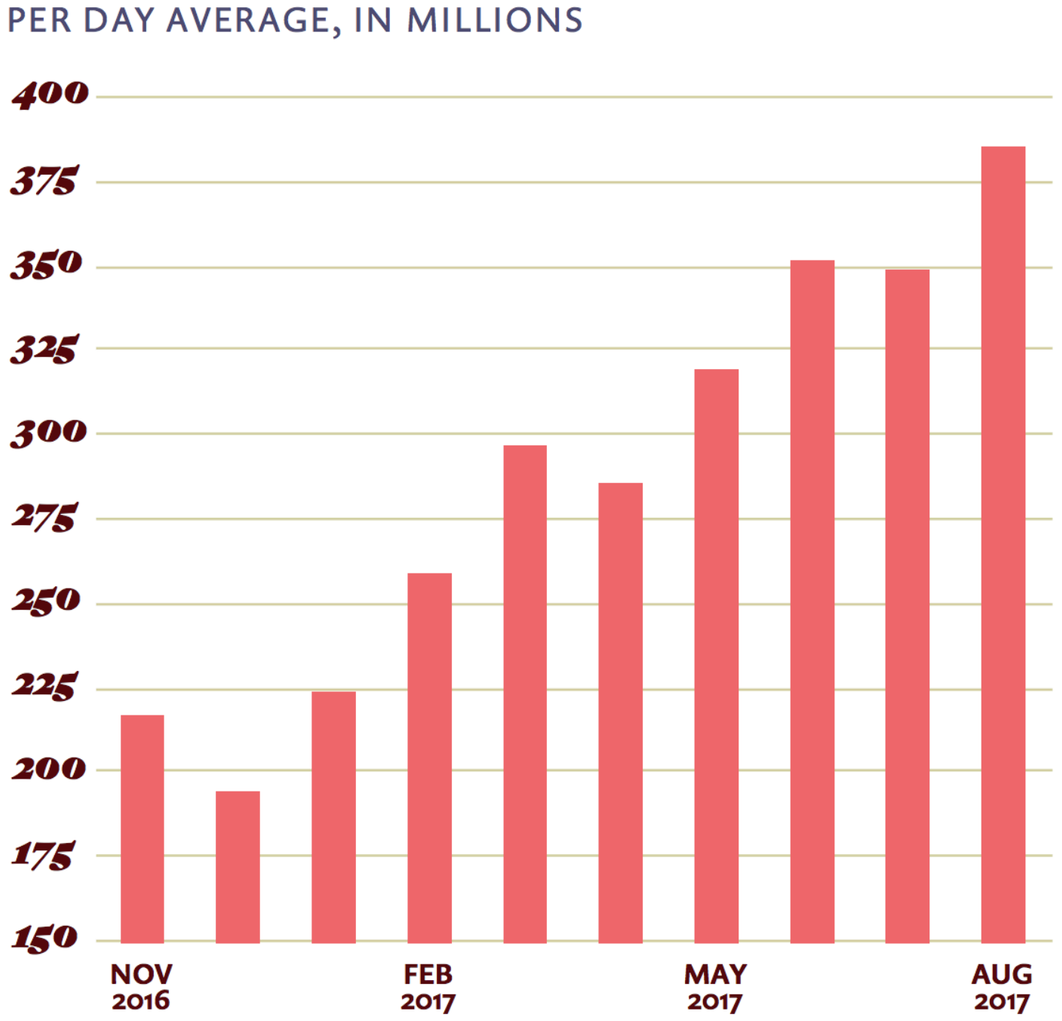
One vulnerability, many victims

Created by snyk

2017

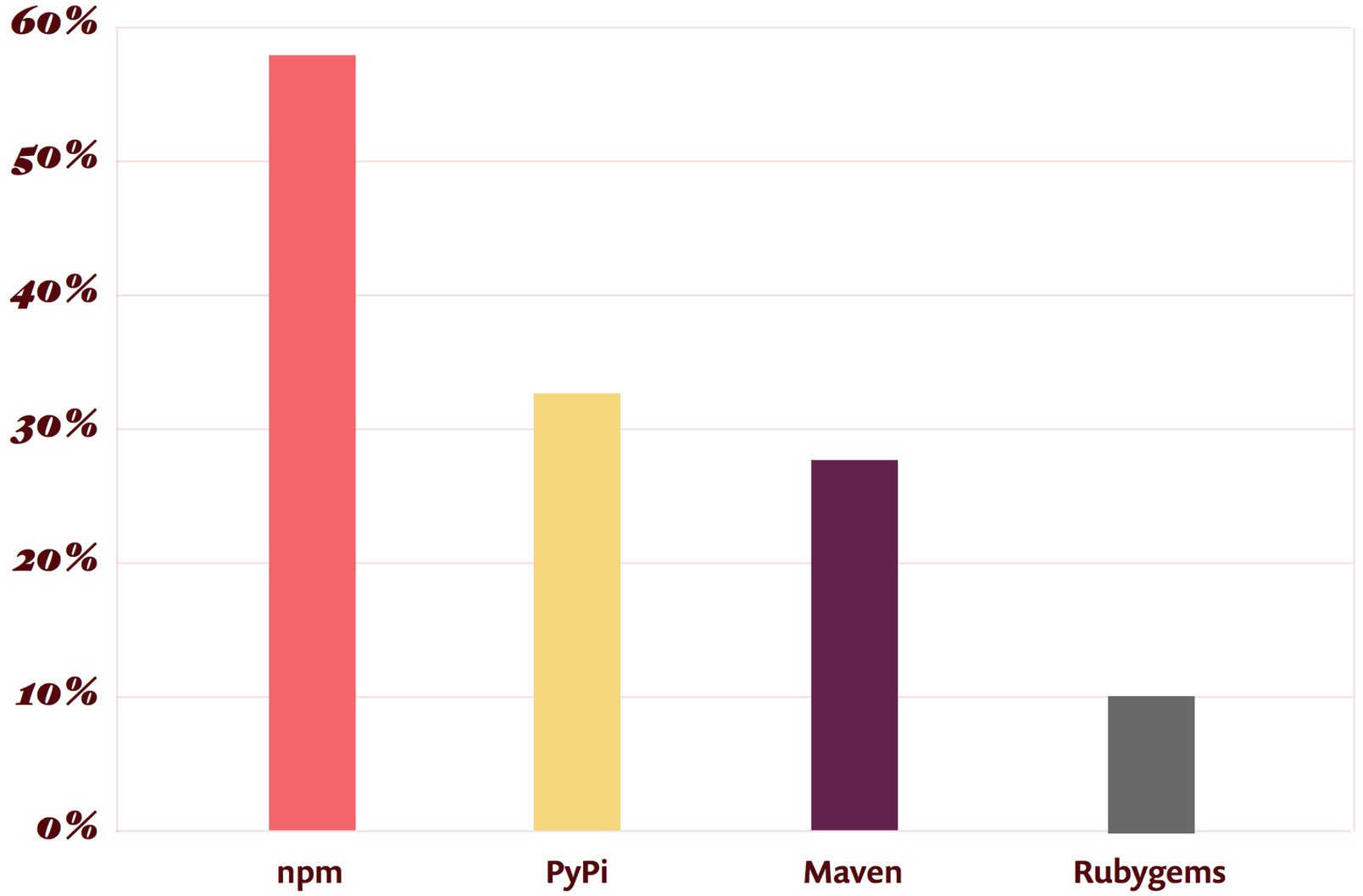
The State of Open Source Security

npm Packages Downloaded, Per Day Average



Percentage Increase in Total Packages Indexed

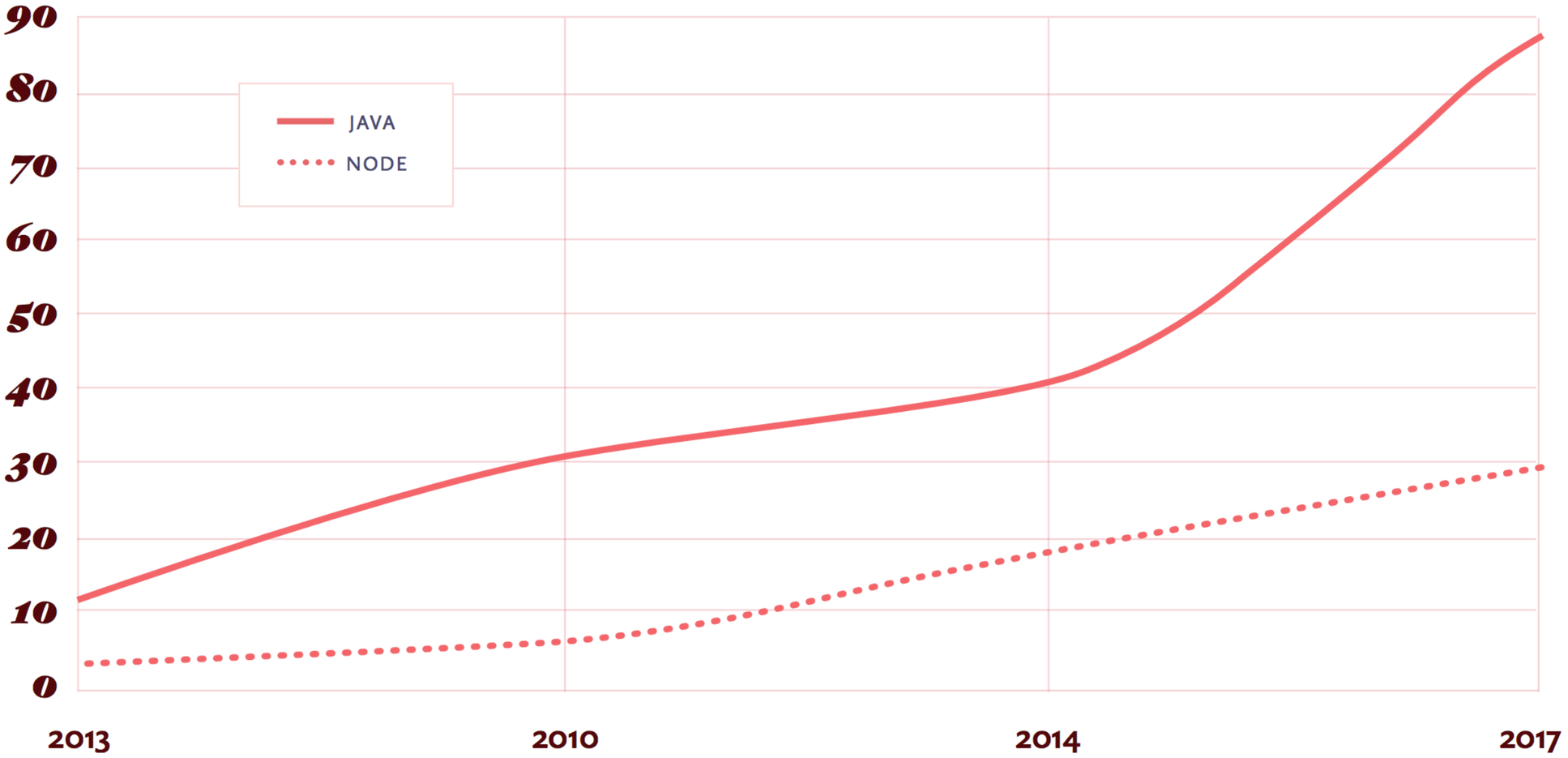
OCTOBER 2016 – OCTOBER 2017



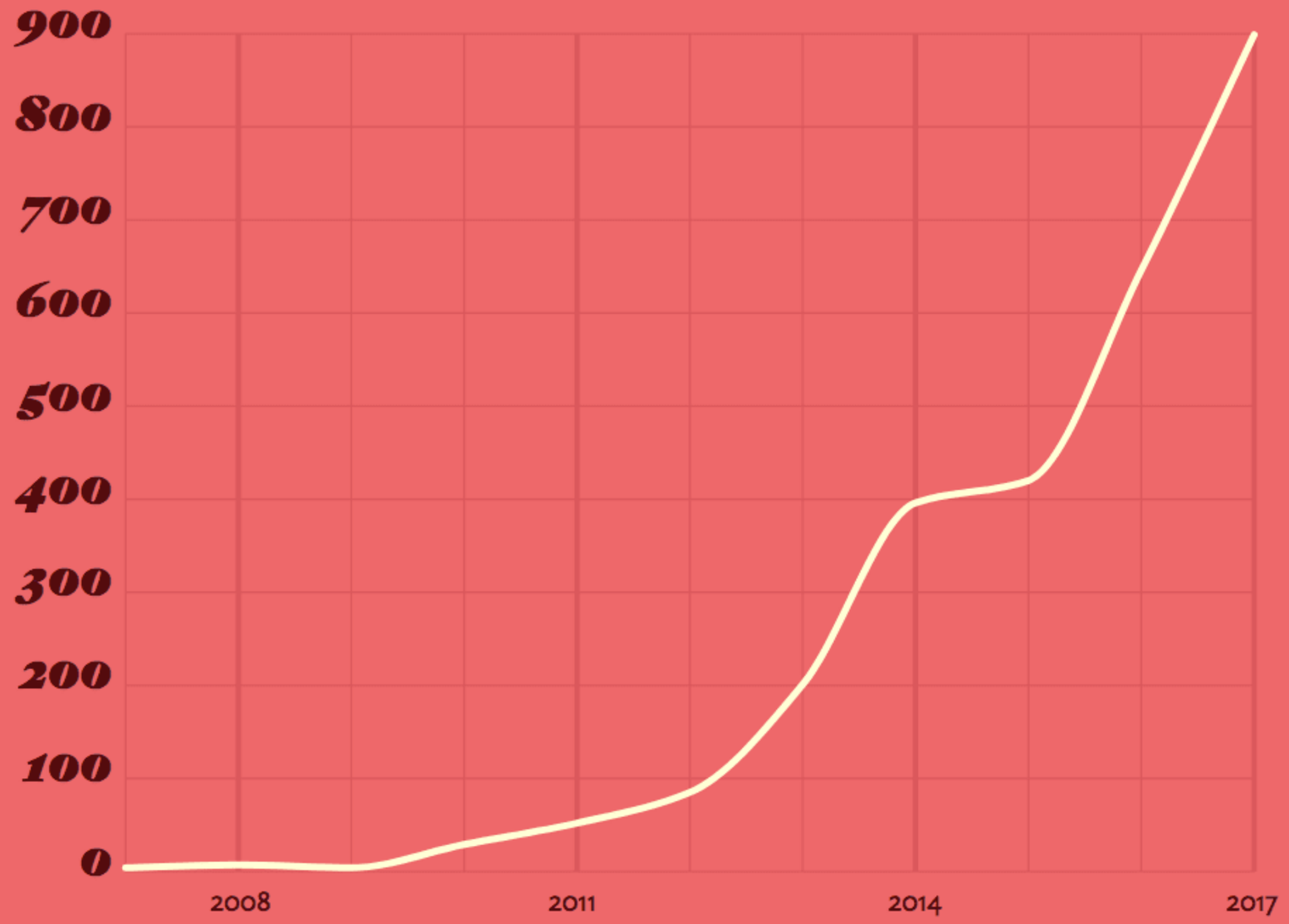
A test of 430,000 sites showed that of them run at least one front-end library with a known security vulnerability.

A test of 430,000 sites showed that *77%* of them run at least one front-end library with a known security vulnerability.

Critical Java & Node Package Vulnerabilities



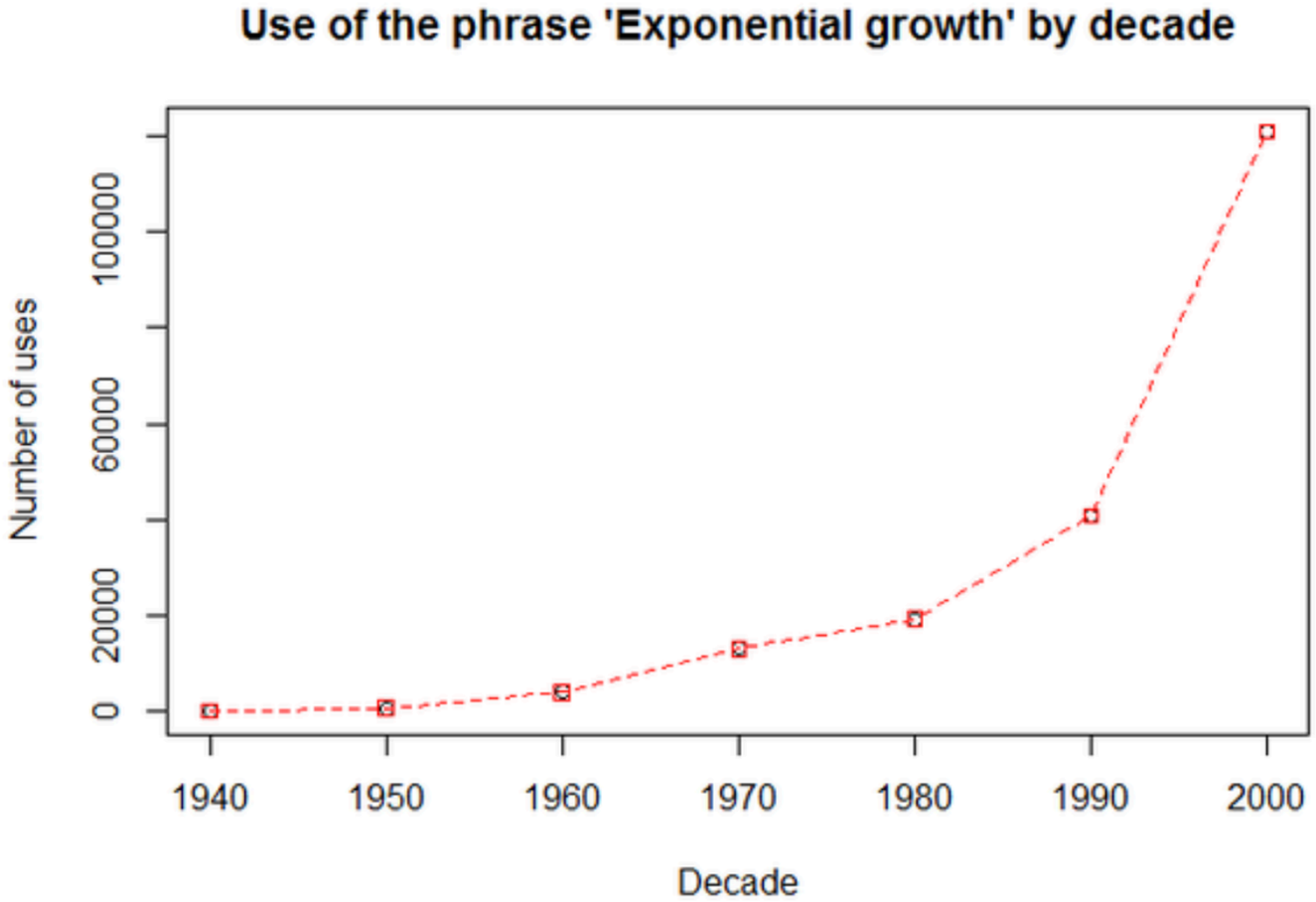
Open Source Vulnerabilities Published Per Year



Matthew Hankins
@mc_hankins

Follow

Use of the phrase 'exponential growth' by decade



Once discovered, maintainers generally react very quickly.

The median time from when a vulnerability is disclosed to when it is fixed:

Once discovered, maintainers generally react very quickly.

The median time from when a vulnerability is disclosed to when it is fixed:

16 days

Vulnerabilities generally remain undiscovered for a long time.

The median time from inclusion to discovery
for in application libraries:

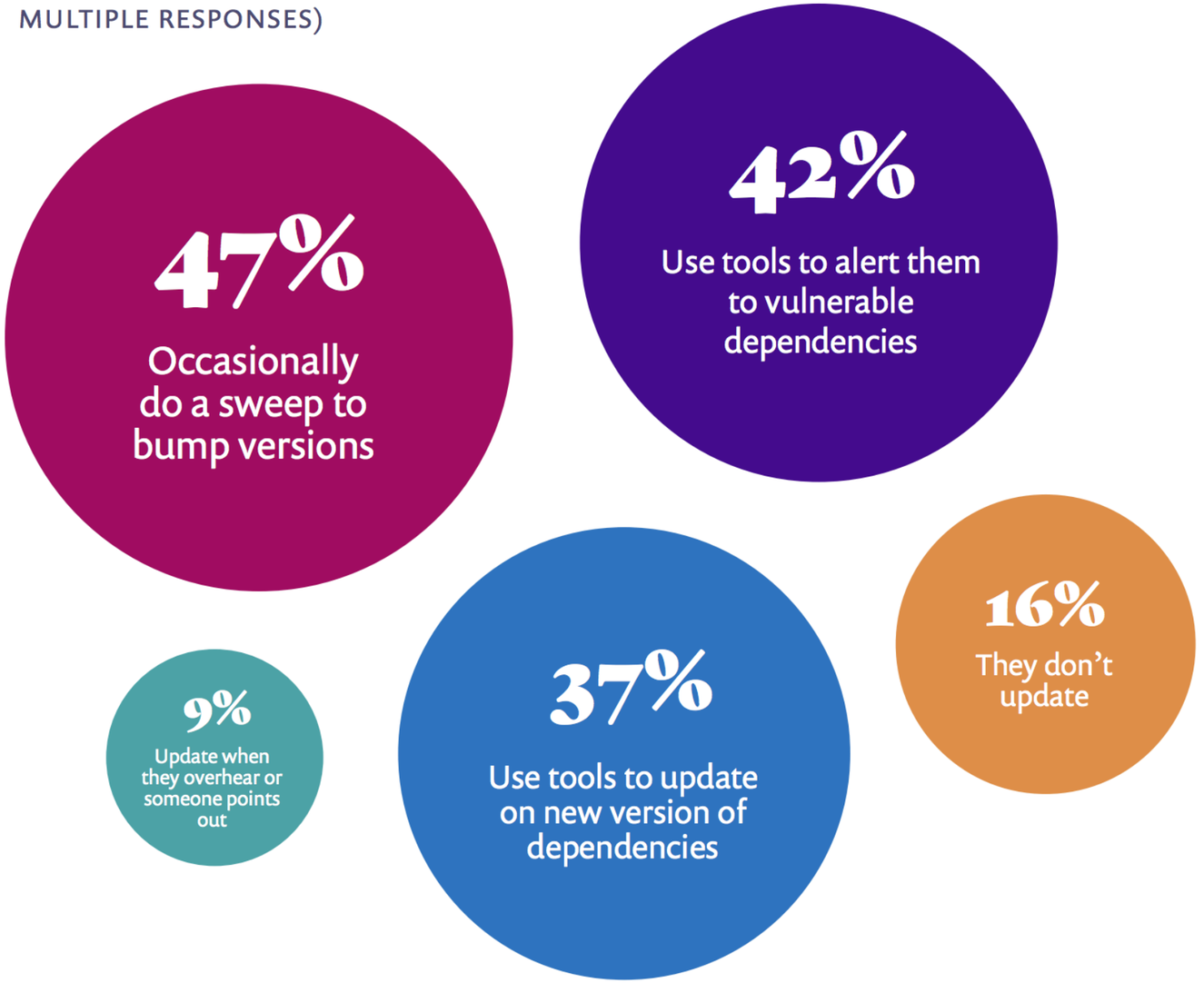
Vulnerabilities generally remain undiscovered for a long time.

The median time from inclusion to discovery for in application libraries:

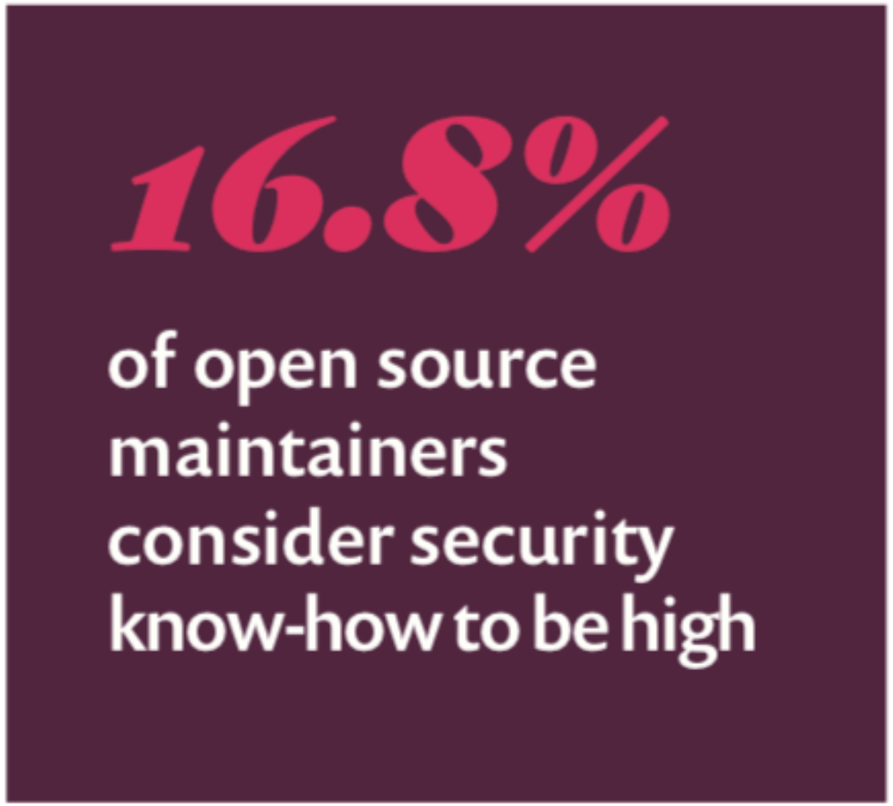
2.5 years

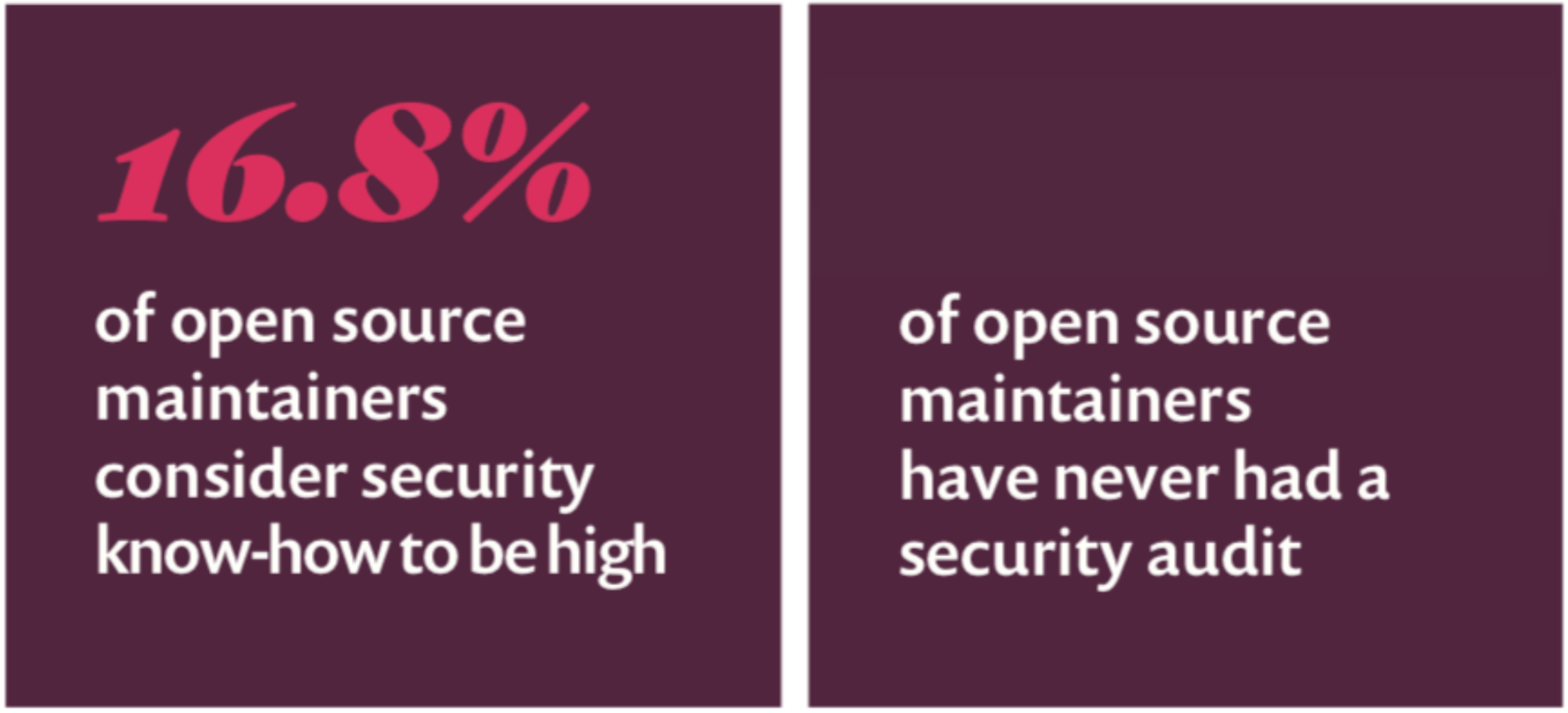
How Do Users Keep Dependencies Up to Date?

(RESPONDENTS WERE ABLE TO SELECT MULTIPLE RESPONSES)



of open source maintainers consider security know-how to be high


16.8%
of open source
maintainers
consider security
know-how to be high

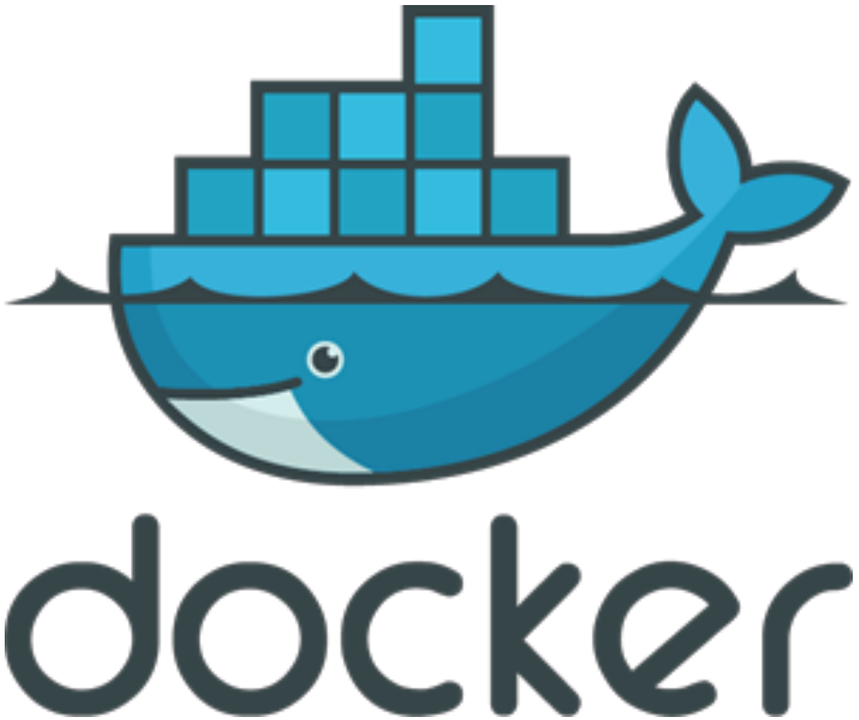

16.8%
of open source maintainers consider security know-how to be high
of open source maintainers have never had a security audit

16.8%

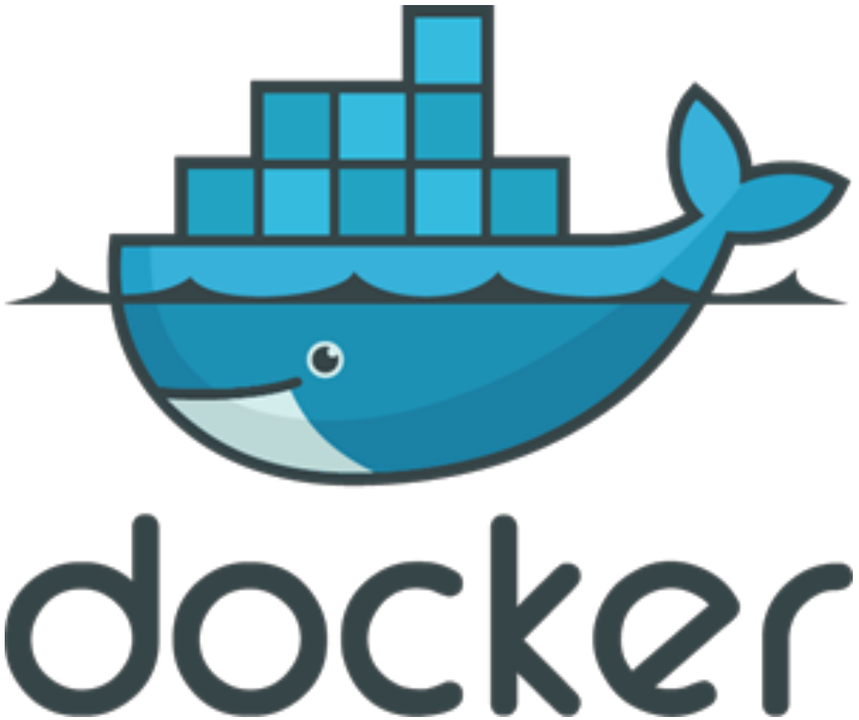
of open source maintainers consider security know-how to be high

43.7%

of open source maintainers have never had a security audit



of the top 1,000
Docker containers
have known
vulnerabilities



76.6%

of the top 1,000 Docker containers have known vulnerabilities

Going Terminal!

What's the **Solution?**

What's the **Solution?**

Team Culture + Process + Tooling

Team Culture

What do people care about?

- Developers
- Security
- Operations
- Management

Process

The **best** way to adopt a **new practice** is to **integrate** it into existing processes, **not create more**.

Tooling

Tooling can **help**

Automate away **manual** steps

Alert you to issues **when** they happen

Security considerations

- Prevention
- Detection
- Response
- Recovery

Questions?

BRIAN VERMEER

BRIANVERMEER@SNYK.IO

@BRIANVERM