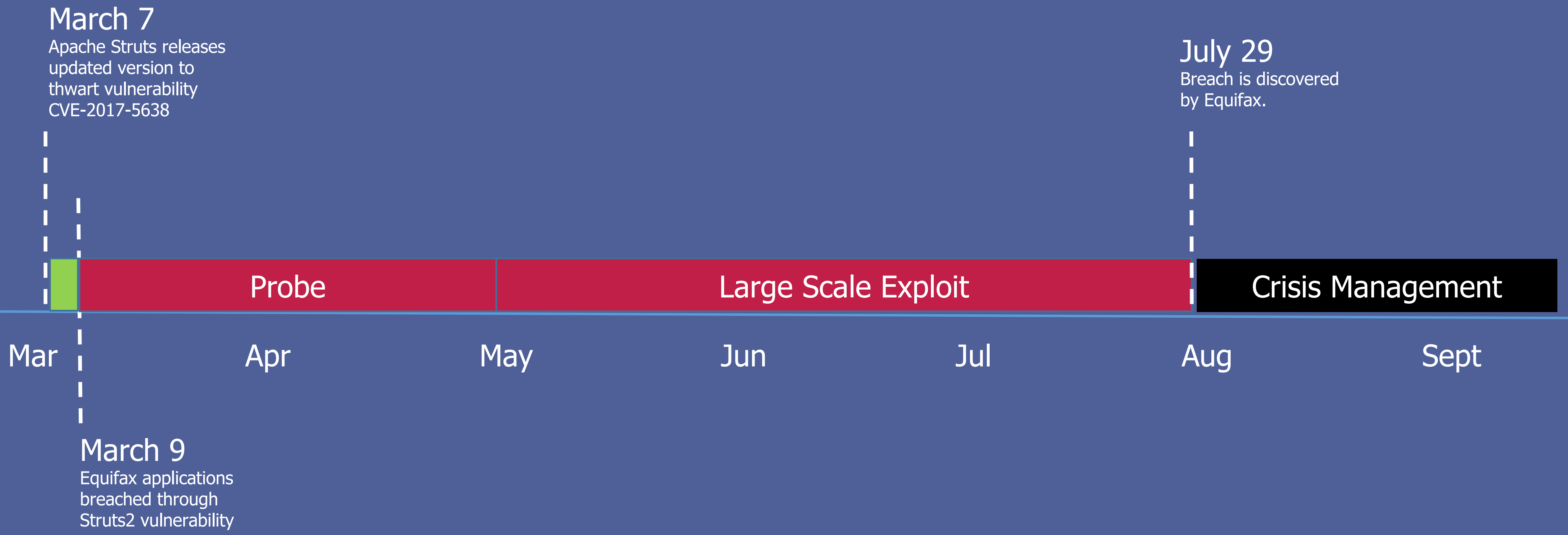
We Are All Equifax: The Data Behind DevSecOps

Stefania Chaplin, EMEA Solutions Engineer

Sonatype

EQUIFAX®



March 7
Apache Struts releases updated version to thwart vulnerability CVE-2017-5638

July 29
Breach is discovered by Equifax.

Probe

Large Scale Exploit

Crisis Management

Mar
Apr
May
Jun
Jul
Aug
Sept

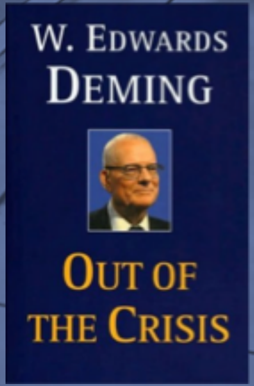
March 9
Equifax applications breached through Struts2 vulnerability

“You cannot inspect quality into a product.”

W. Edwards Deming

Out of the Crisis

1982

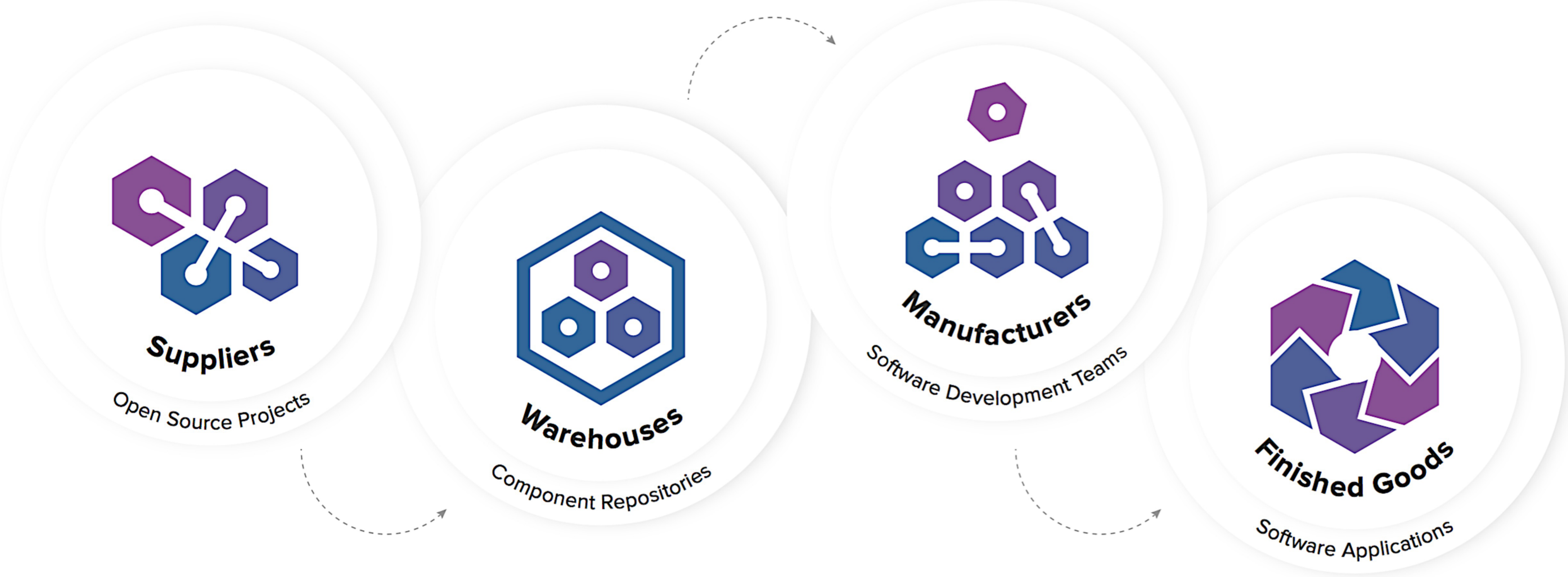


W. EDWARDS DEMING

OUT OF THE CRISIS

2017 STATE OF THE SOFTWARE SUPPLY CHAIN

Say Hello to Your Software Supply Chain…



Suppliers

Open Source Projects

Warehouses

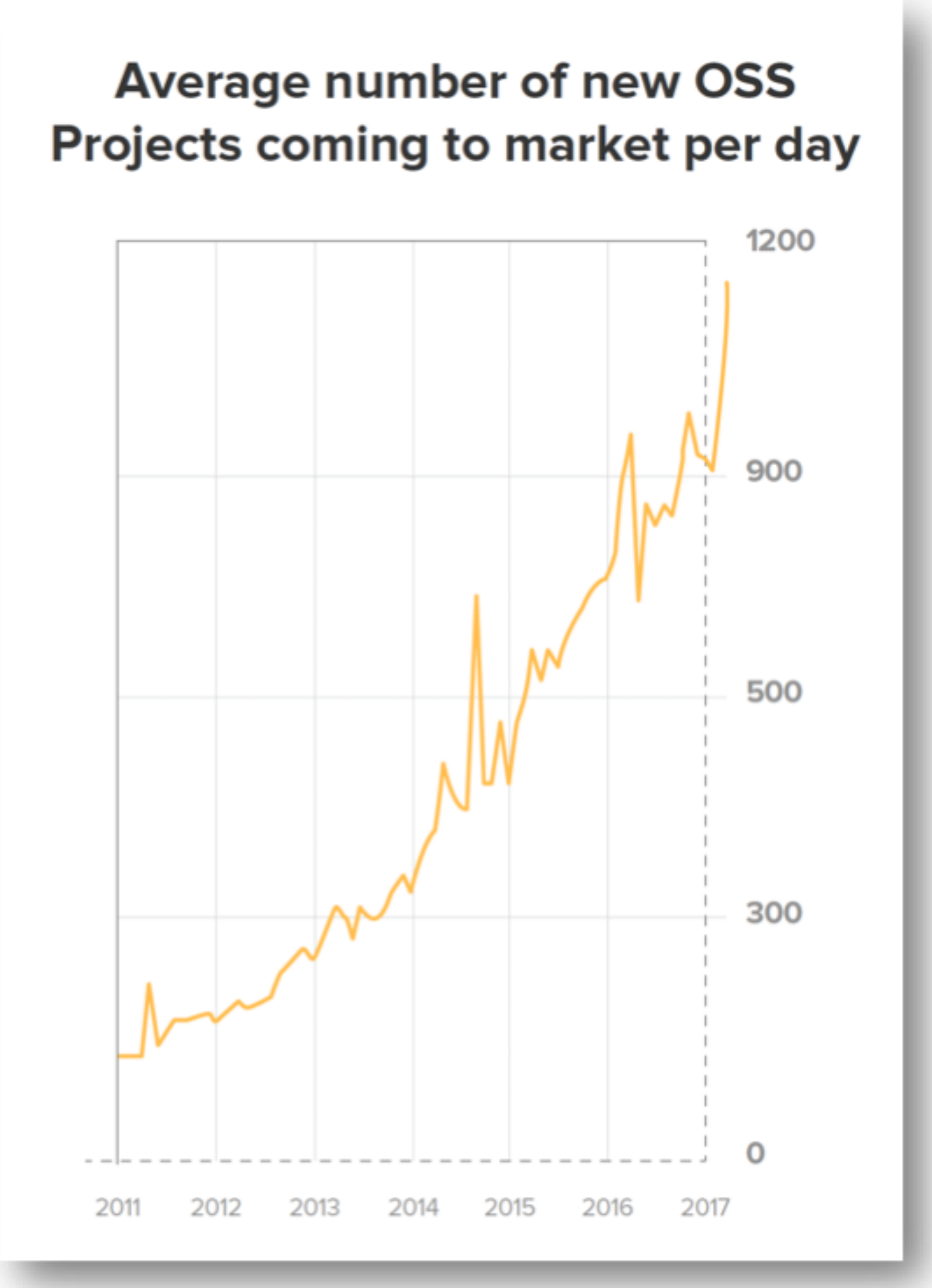
Component Repositories

Manufacturers

Software Development Teams

Finished Goods

Software Applications



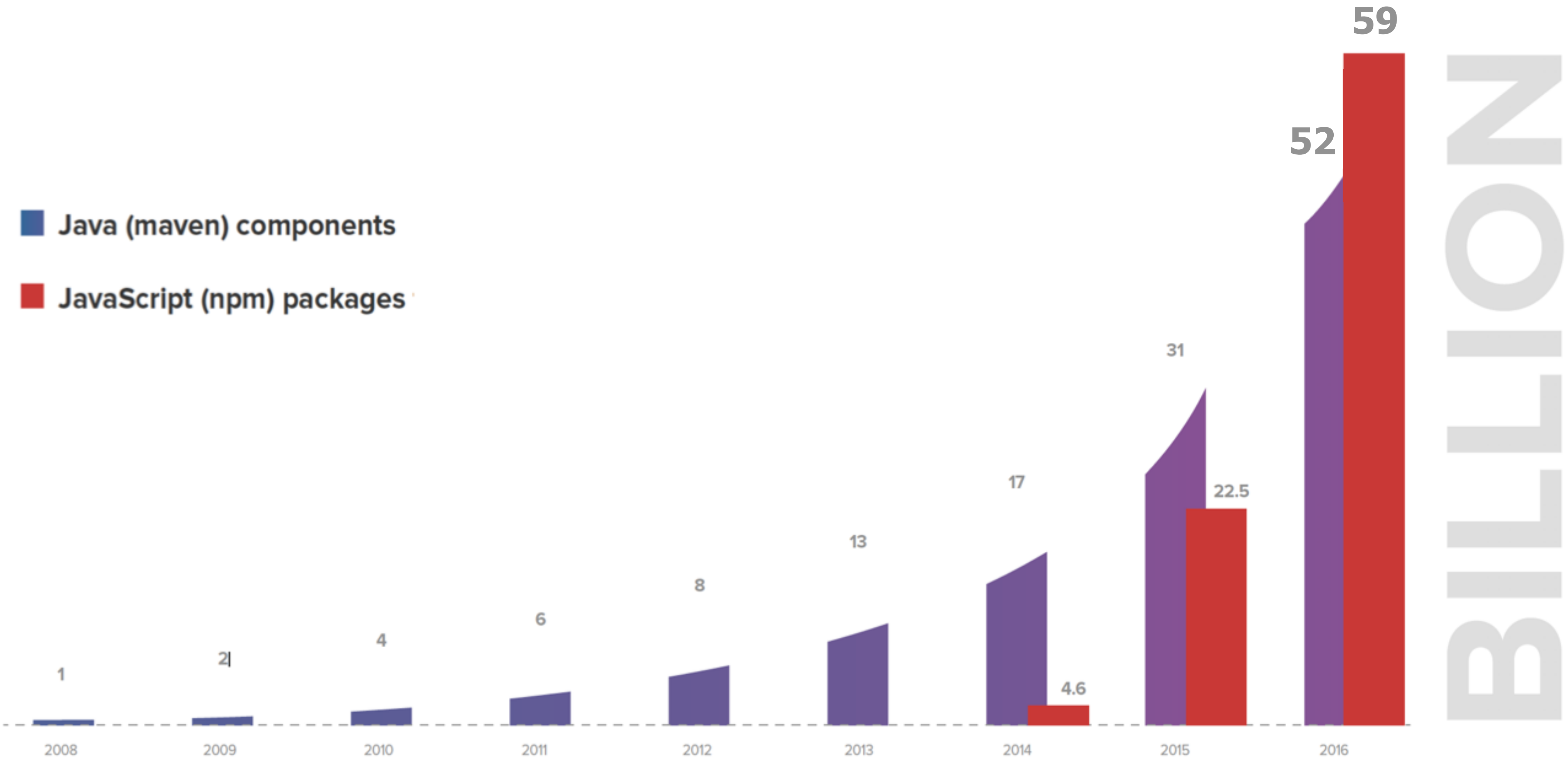
1,096 new projects per day

10,000 new versions per day

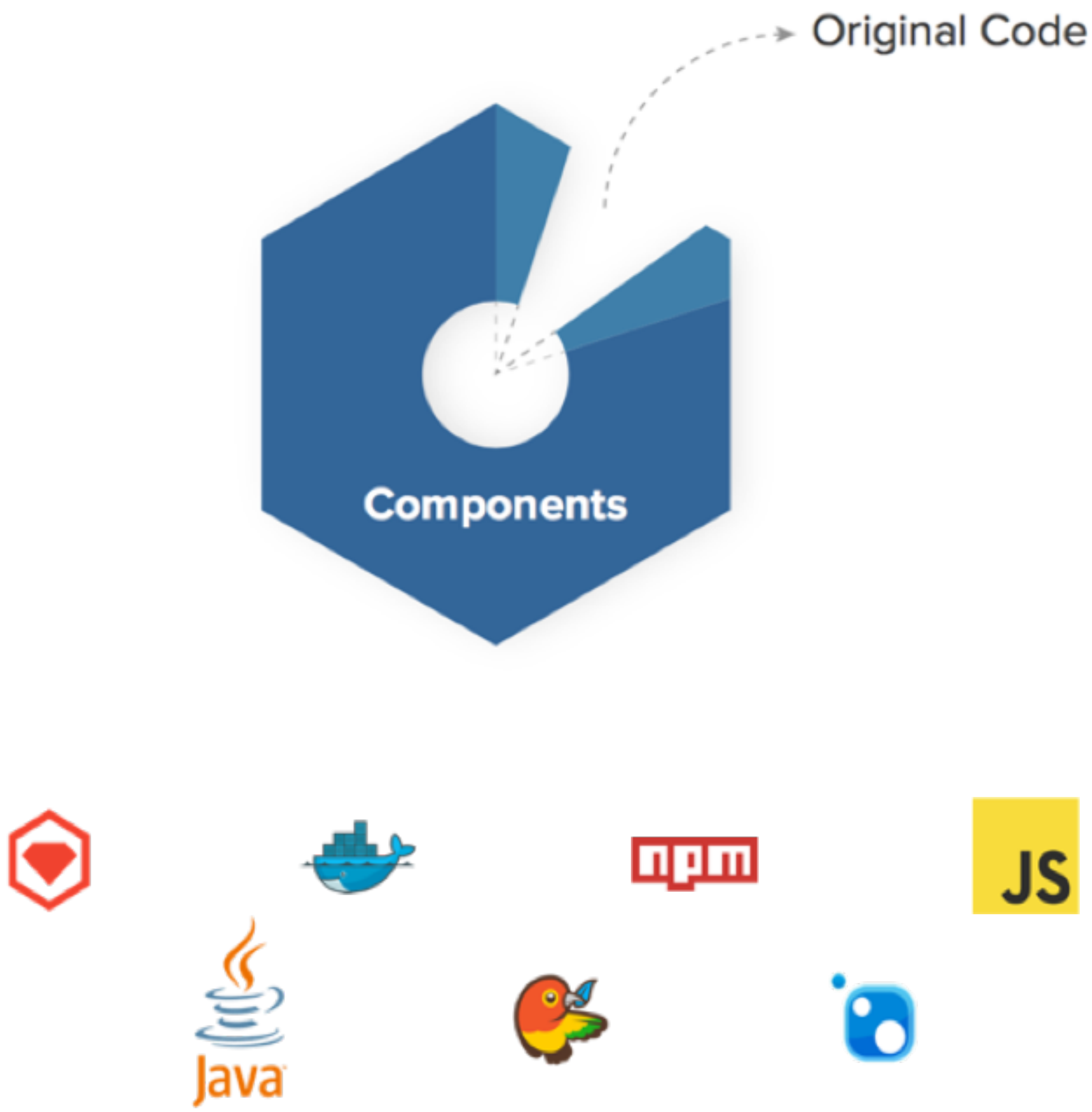
14x releases per year

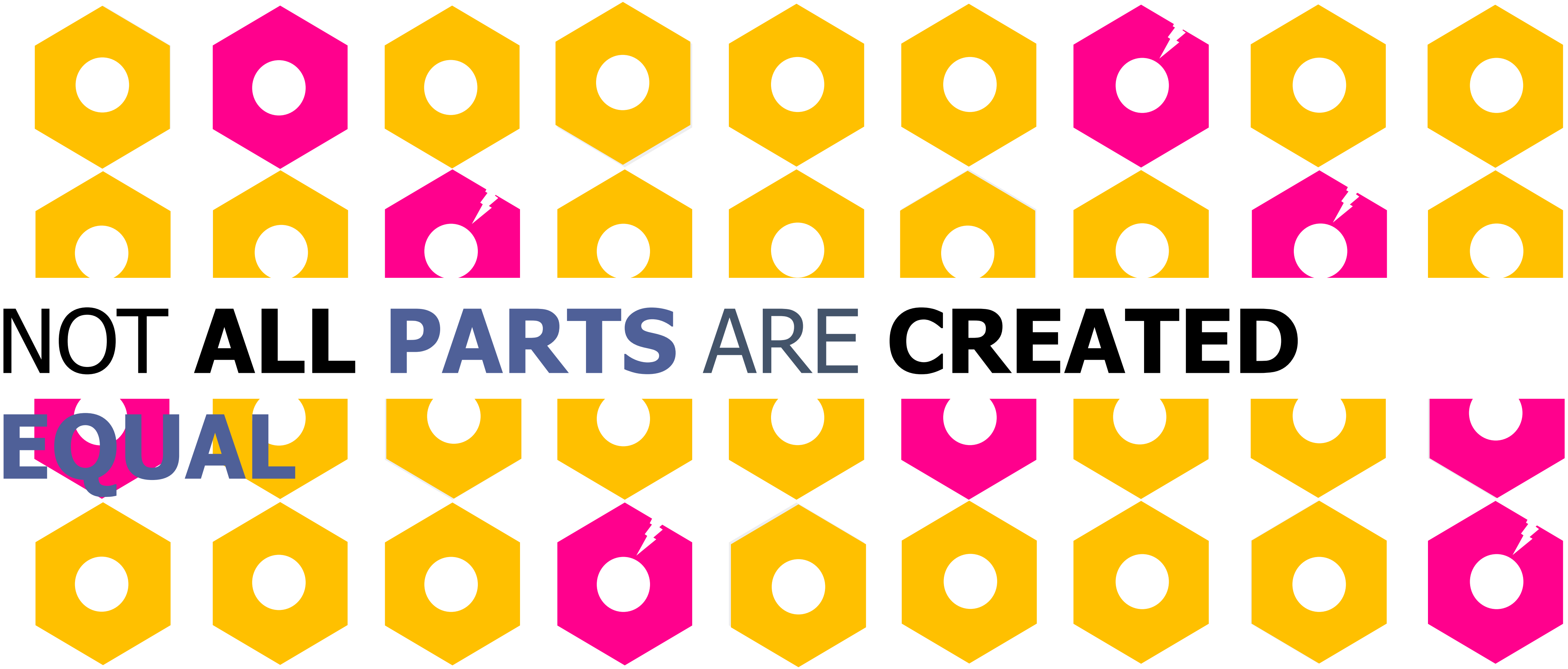
- 3M npm components
- 2M Java components

- 900K NuGet components
- 870K PyPI components


Java (maven) components
JavaScript (npm) packages
1
2
4
6
8
13
17
4.6
31
22.5
52
59
BILLION
2008
2009
2010
2011
2012
2013
2014
2015
2016

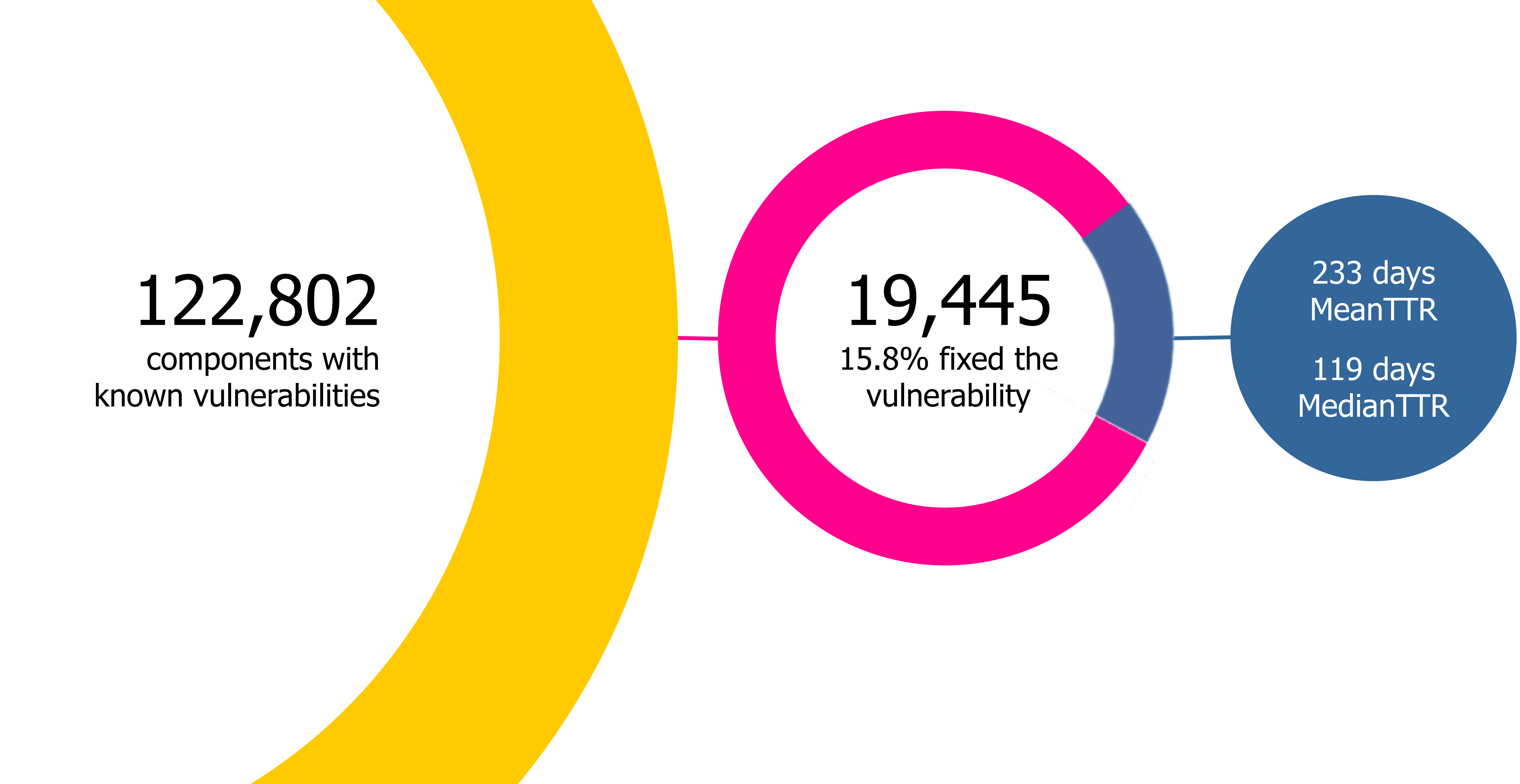
80% to 90% of **modern apps** consist of assembled components.





NOT **ALL PARTS** ARE **CREATED EQUAL**

TIME TO REPAIR OSS COMPONENTS



122,802
components with
known vulnerabilities

19,445
15.8% fixed the
vulnerability

233 days
MeanTTR

119 days
MedianTTR

BOUNCY CASTLE

2007

CVE-2007-6721
CVSS Base Score: 10.0 HIGH
Exploitability Subscore: 10.0

23M

2016

9 years later, vulnerable versions of Bouncy Castle were downloaded…

11M

COMMONS **COLLECTION**

CWE-502

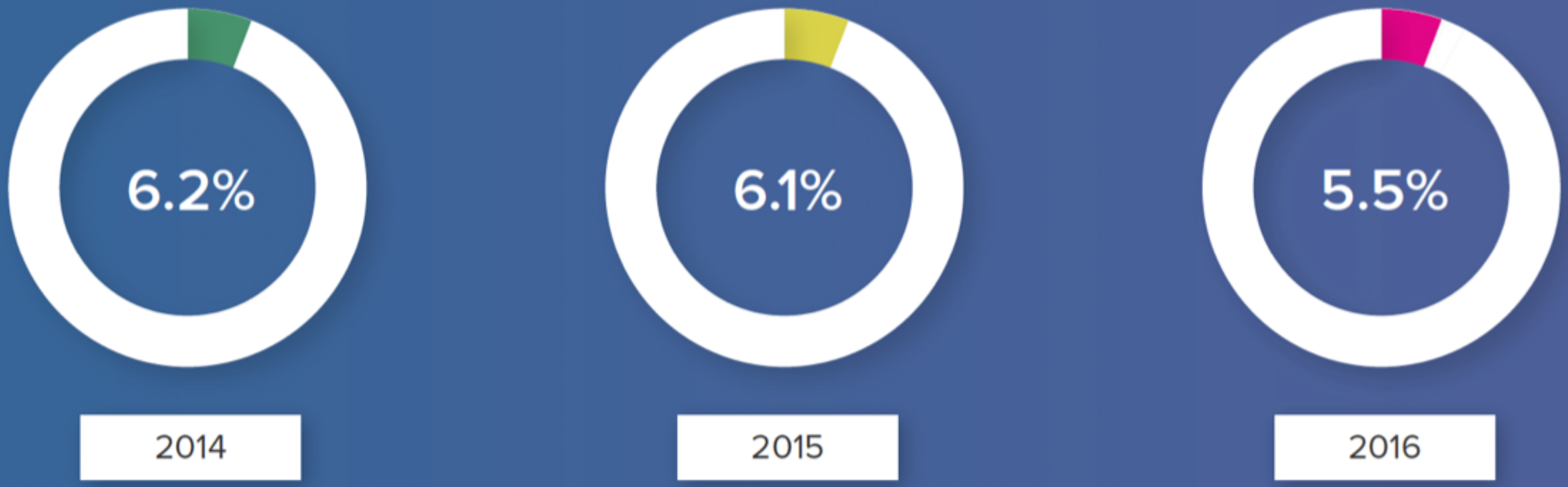
23,476,966

total downloads in 2016

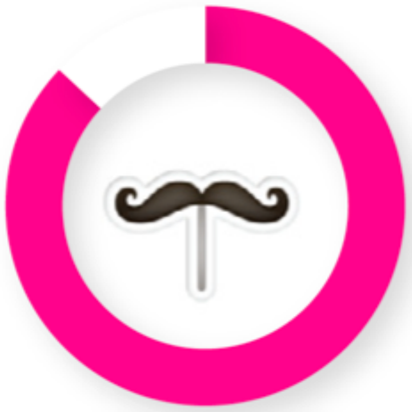
18,330,958

78% downloads were vulnerable

In 2016, the defect download ratio for Java components was 1-in-18

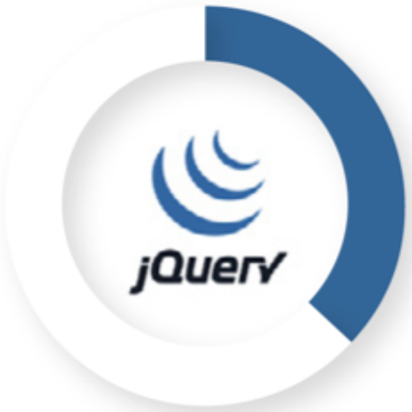


DEFECT **PERCENTAGES** **FOR** JAVASCRIPT



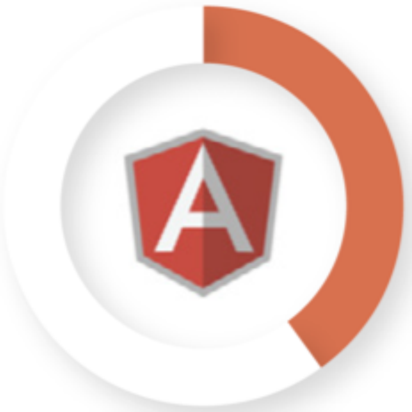
87%

of Handlebars inclusions were known vulnerable



37%

of jQuery inclusions were known vulnerable

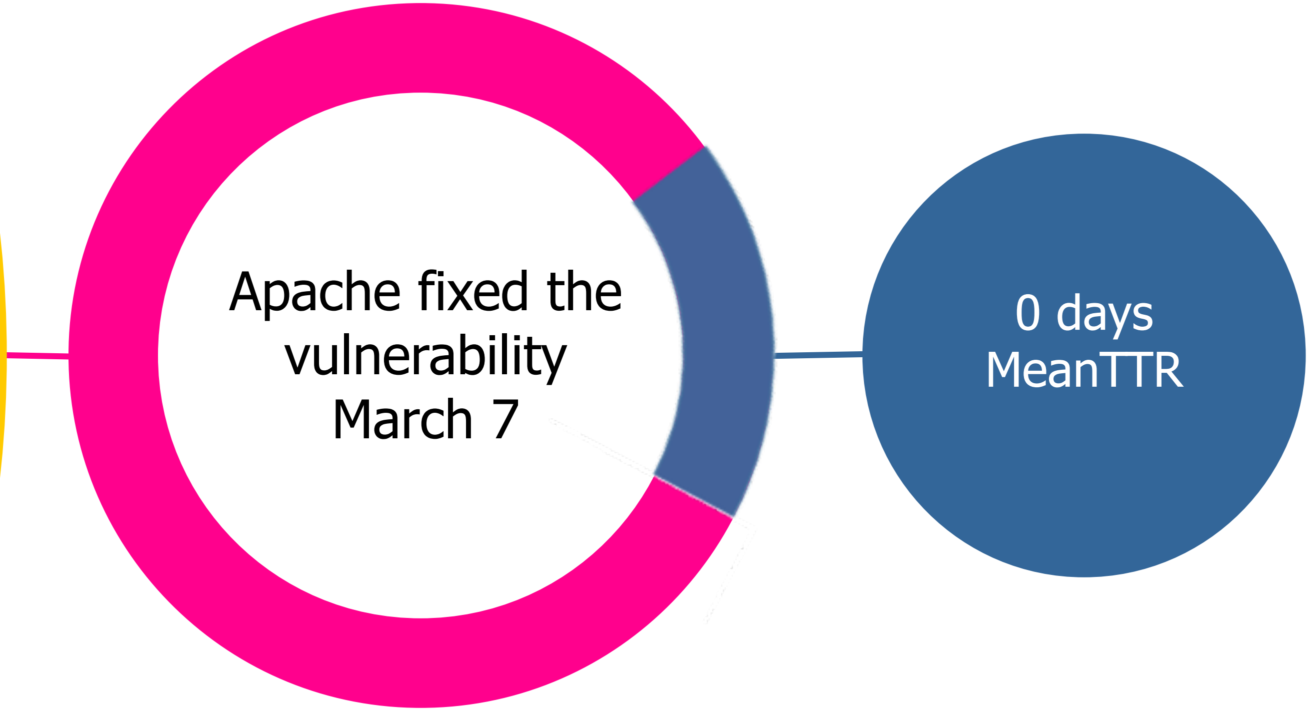


40%

of Angular inclusions were known vulnerable

APACHE STRUTS2 MEAN TIME TO REPAIR

CVE ID: CVE-2017-5638
March 7

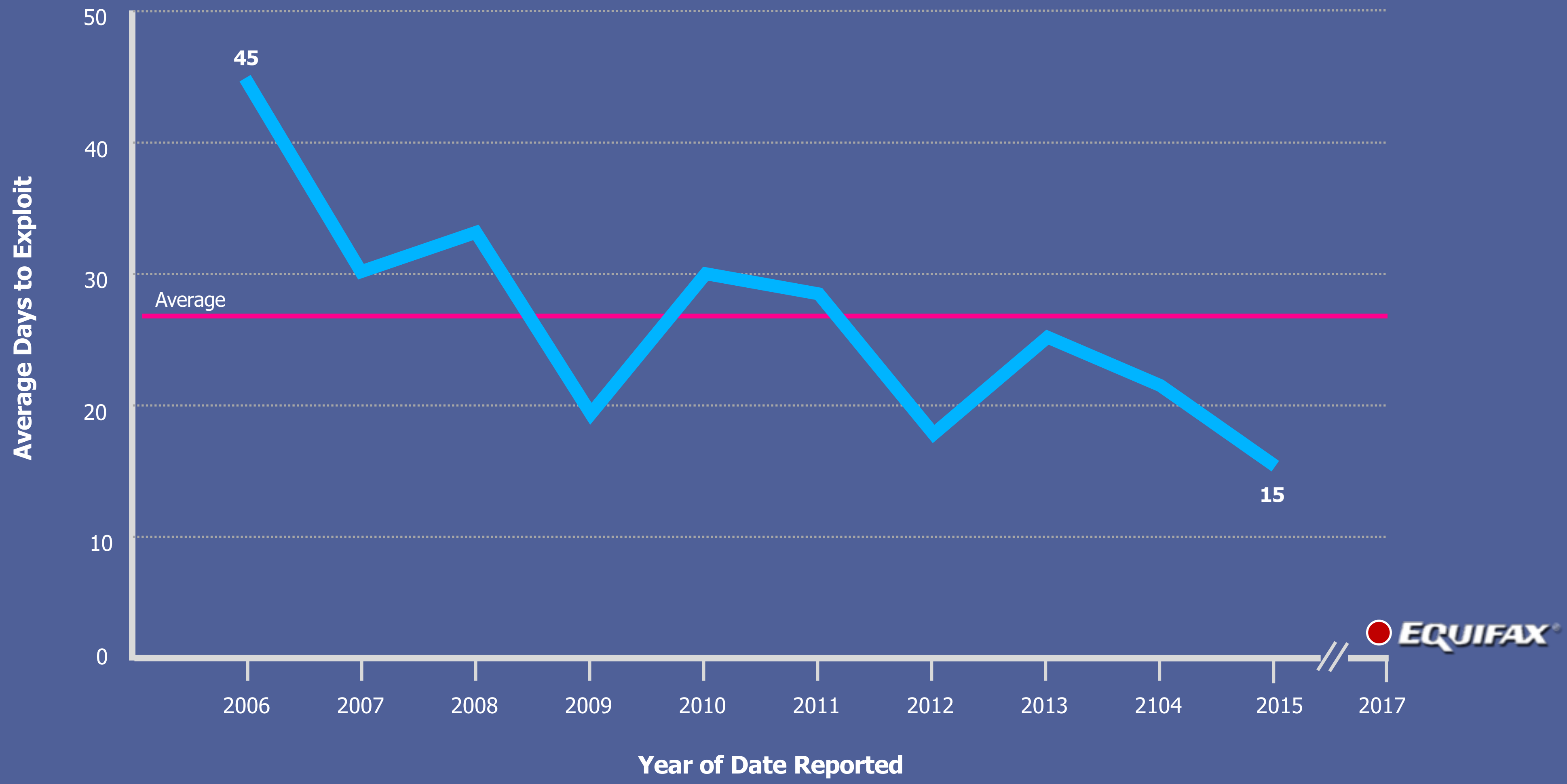


Apache fixed the vulnerability
March 7

0 days
MeanTTR

TIME TO RESPOND BEFORE EXPLOIT

Source: Adapted from IBM X-Force / Analysis by Gartner Research (September 2016)

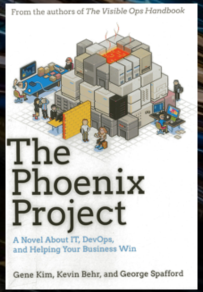


"Emphasize performance of the entire system and never pass a defect downstream."

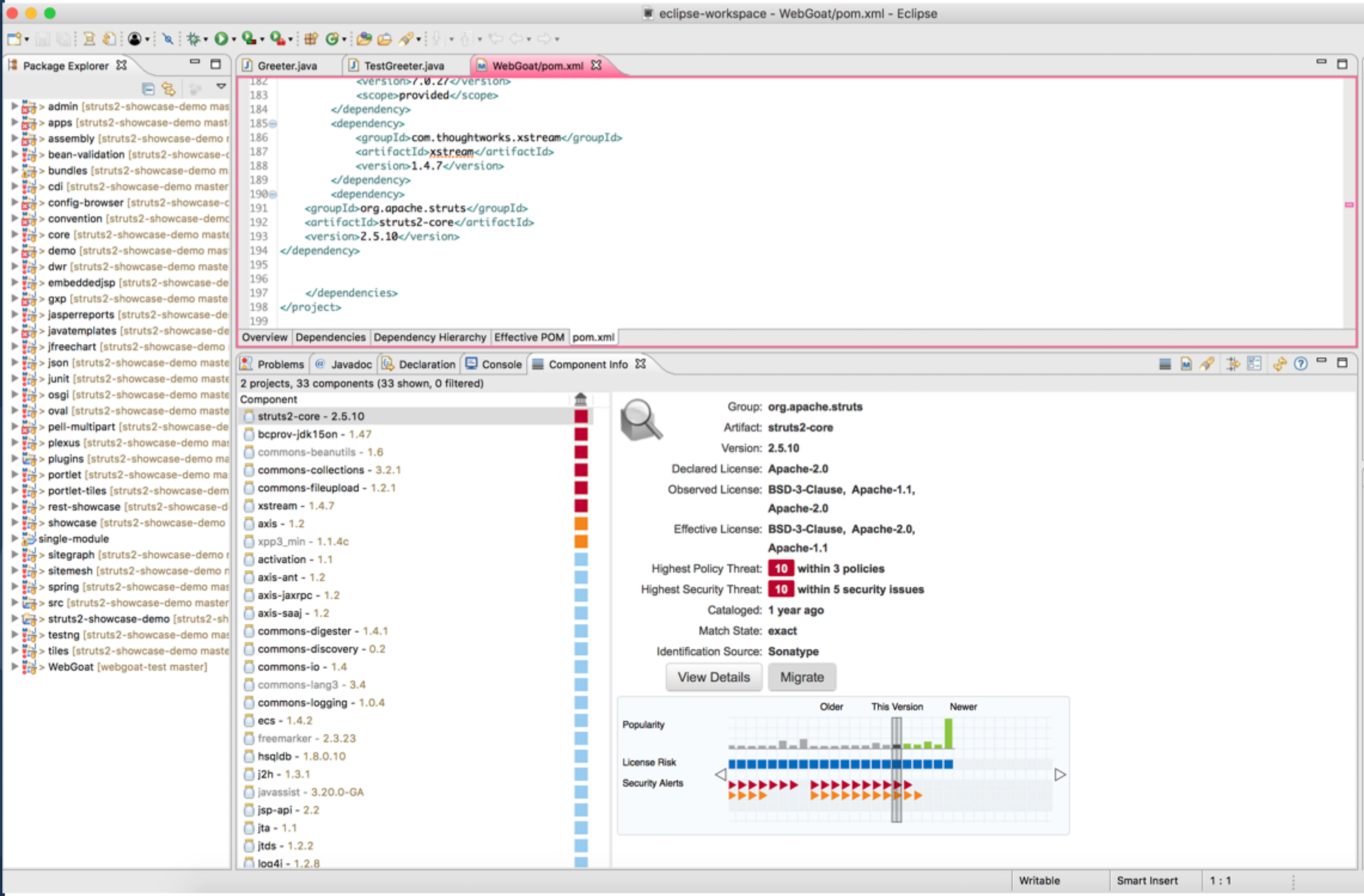
Gene Kim

The Phoenix Project

2013


From the authors of The Visible Ops Handbook
The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
Gene Kim, Kevin Behr, and George Spafford

Early Visibility



eclipse-workspace - WebGoat/pom.xml - Eclipse

- admin [struts2-showcase-demo mas
- apps [struts2-showcase-demo mast
- assembly [struts2-showcase-demo r
- bean-validation [struts2-showcase-c
- bundles [struts2-showcase-demo m
- cdi [struts2-showcase-demo master
- config-browser [struts2-showcase-c
- convention [struts2-showcase-demo
- core [struts2-showcase-demo maste
- demo [struts2-showcase-demo mas
- dwr [struts2-showcase-demo maste
- embeddedjsp [struts2-showcase-de
- gxp [struts2-showcase-demo maste
- jasperreports [struts2-showcase-de
- javatemplates [struts2-showcase-de
- jfreechart [struts2-showcase-demo
- json [struts2-showcase-demo maste
- junit [struts2-showcase-demo maste
- osgi [struts2-showcase-demo maste
- oval [struts2-showcase-demo maste
- pell-multipart [struts2-showcase-de
- plexus [struts2-showcase-demo mas
- plugins [struts2-showcase-demo ma
- portlet [struts2-showcase-demo ma
- portlet-tiles [struts2-showcase-dem
- rest-showcase [struts2-showcase-d
- showcase [struts2-showcase-demo
- single-module
- sitegraph [struts2-showcase-demo r
- sitemesh [struts2-showcase-demo n
- spring [struts2-showcase-demo mas
- src [struts2-showcase-demo master
- struts2-showcase-demo [struts2-sh
- testng [struts2-showcase-demo mas
- tiles [struts2-showcase-demo maste
- WebGoat [webgoat-test master]

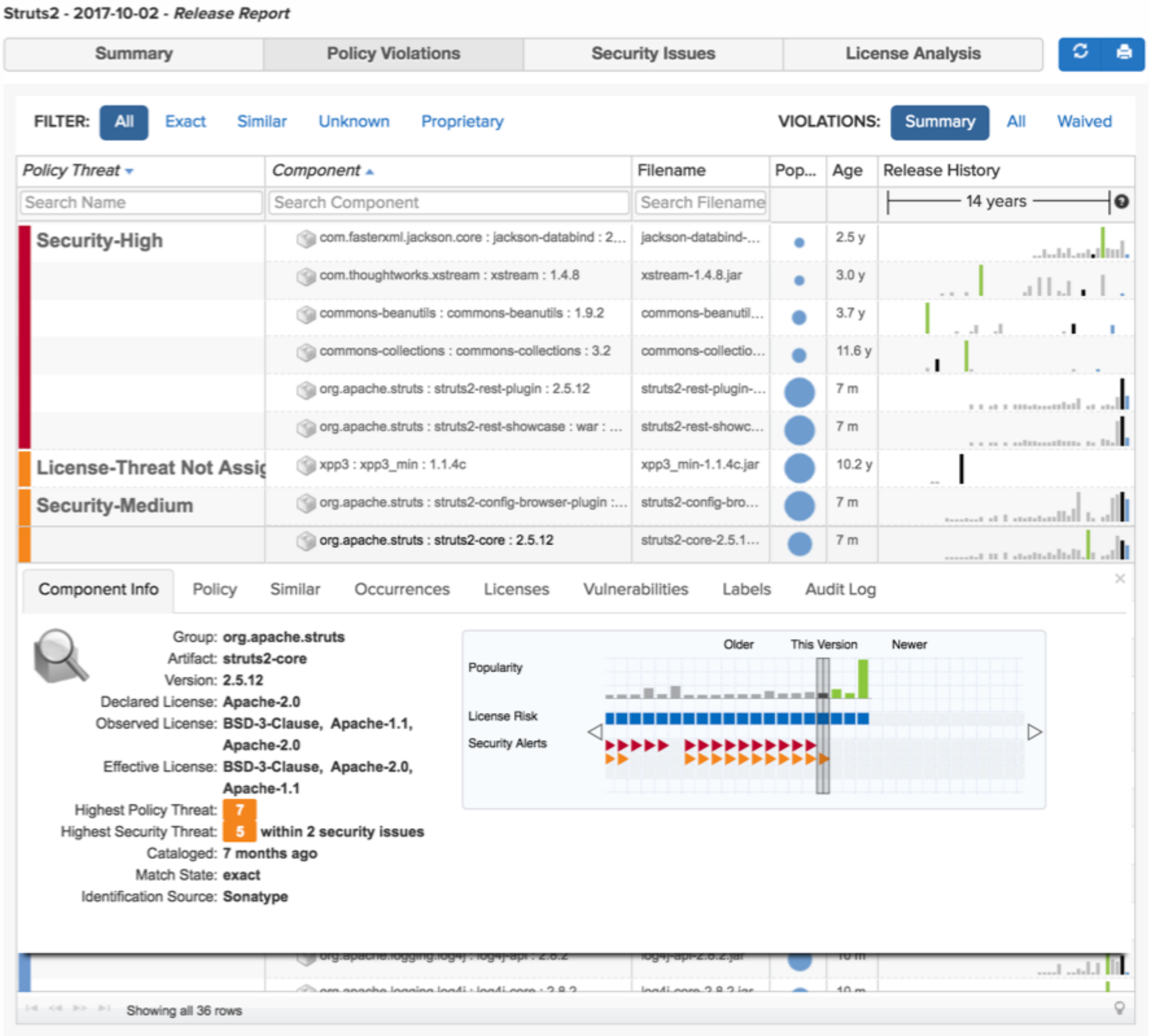
```
                <version>7.0.27</version>
                <scope>provided</scope>
            </dependency>
            <dependency>
                <groupId>com.thoughtworks.xstream</groupId>
                <artifactId>xstream</artifactId>
                <version>1.4.7</version>
            </dependency>
            <dependency>
        <groupId>org.apache.struts</groupId>
        <artifactId>struts2-core</artifactId>
        <version>2.5.10</version>
    </dependency>


        </dependencies>
    </project>
```

2 projects, 33 components (33 shown, 0 filtered)

Component	
struts2-core - 2.5.10	🟥
bcprov-jdk15on - 1.47	🟥
commons-beanutils - 1.6	🟥
commons-collections - 3.2.1	🟥
commons-fileupload - 1.2.1	🟥
xstream - 1.4.7	🟥
axis - 1.2	🟧
xpp3_min - 1.1.4c	🟧
activation - 1.1	🟦
axis-ant - 1.2	🟦
axis-jaxrpc - 1.2	🟦
axis-saaj - 1.2	🟦
commons-digester - 1.4.1	🟦
commons-discovery - 0.2	🟦
commons-io - 1.4	🟦
commons-lang3 - 3.4	🟦
commons-logging - 1.0.4	🟦
ecs - 1.4.2	🟦
freemarker - 2.3.23	🟦
hsqldb - 1.8.0.10	🟦
j2h - 1.3.1	🟦
javassist - 3.20.0-GA	🟦
jsp-api - 2.2	🟦
jta - 1.1	🟦
jtds - 1.2.2	🟦
log4j - 1.2.8	🟦

Group: org.apache.struts
Artifact: struts2-core
Version: 2.5.10
Declared License: Apache-2.0
Observed License: BSD-3-Clause, Apache-1.1, Apache-2.0
Effective License: BSD-3-Clause, Apache-2.0, Apache-1.1
Highest Policy Threat: 10 within 3 policies
Highest Security Threat: 10 within 5 security issues
Cataloged: 1 year ago
Match State: exact
Identification Source: Sonatype

Software Bill of Materials



Struts2 - 2017-10-02 - *Release Report*

FILTER: All Exact Similar Unknown Proprietary

VIOLATIONS: Summary All Waived

Policy Threat	*Component*	Filename	Pop...	Age	Release History
Search Name	Search Component	Search Filename			14 years
Security-High	com.fasterxml.jackson.core : jackson-databind : 2...	jackson-databind-...	●	2.5 y	
	com.thoughtworks.xstream : xstream : 1.4.8	xstream-1.4.8.jar	●	3.0 y	
	commons-beanutils : commons-beanutils : 1.9.2	commons-beanutil...	●	3.7 y	
	commons-collections : commons-collections : 3.2	commons-collectio...	●	11.6 y	
	org.apache.struts : struts2-rest-plugin : 2.5.12	struts2-rest-plugin-...	●	7 m	
	org.apache.struts : struts2-rest-showcase : war : ...	struts2-rest-showc...	●	7 m	
License-Threat Not Assig	xpp3 : xpp3_min : 1.1.4c	xpp3_min-1.1.4c.jar	●	10.2 y	
Security-Medium	org.apache.struts : struts2-config-browser-plugin :...	struts2-config-bro...	●	7 m	
	org.apache.struts : struts2-core : 2.5.12	struts2-core-2.5.1...	●	7 m	

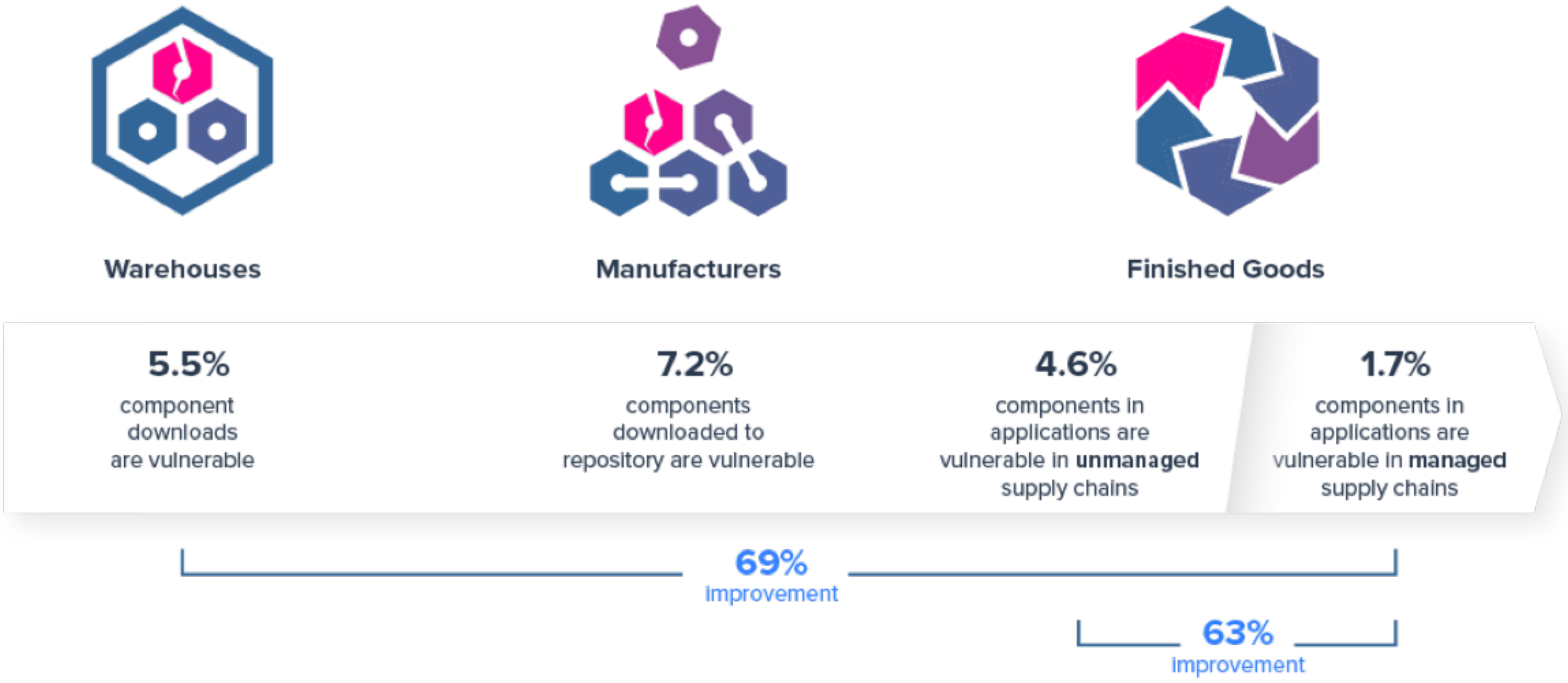
Group: org.apache.struts
Artifact: struts2-core
Version: 2.5.12
Declared License: Apache-2.0
Observed License: BSD-3-Clause, Apache-1.1, Apache-2.0
Effective License: BSD-3-Clause, Apache-2.0, Apache-1.1
Highest Policy Threat: 7
Highest Security Threat: 5 within 2 security issues
Cataloged: 7 months ago
Match State: exact
Identification Source: Sonatype

	org.apache.logging.log4j : log4j-api : 2.8.2	log4j-api-2.8.2.jar	●	10 m	
	org.apache.logging.log4j : log4j-core : 2.8.2	log4j-core-2.8.2.jar	●	10 m	

Showing all 36 rows

Sonatype

TRUSTED SOFTWARE SUPPLY CHAINS



Warehouses

Manufacturers

Finished Goods

5.5%
component downloads are vulnerable

7.2%
components downloaded to repository are vulnerable

4.6%
components in applications are vulnerable in **unmanaged** supply chains

1.7%
components in applications are vulnerable in **managed** supply chains

69%
improvement

63%
improvement

THE **REWARDS** ARE **IMPRESSIVE**

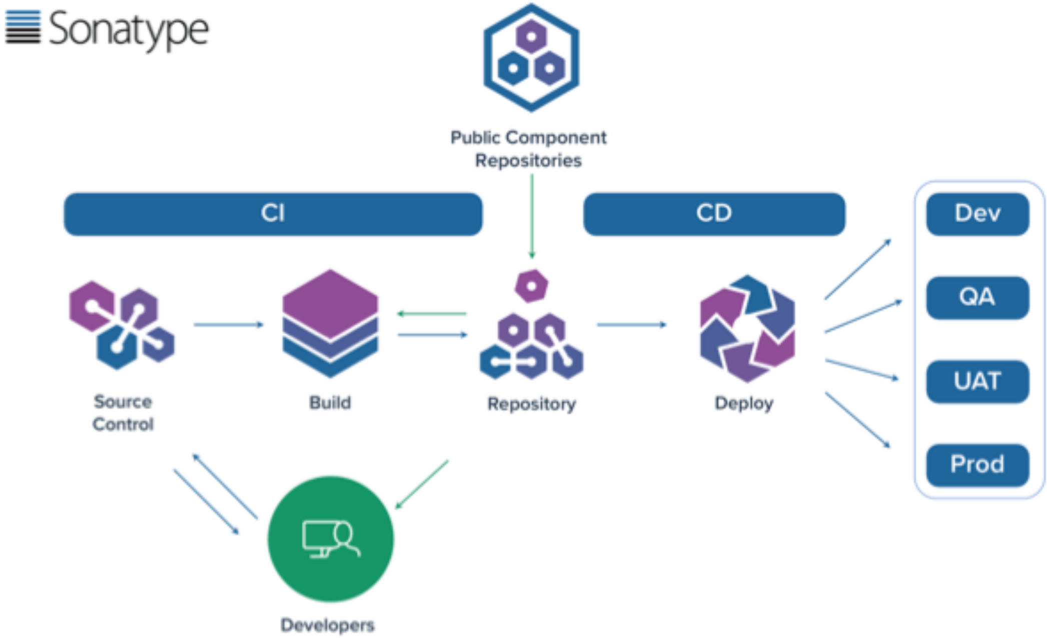
90%
improvement in time to deploy

34,000
hours saved in
90 days

48%
increase in application quality

Three Takeaways

1. Have a Software BoM for each application so you know what OSS you are using
2. Shift Left! Empower developers by giving them information into their IDEs
3. Add checks at every stage to ensure you don't pass defects downstream



Step 1 - Create your own BoM

PREMIUM

Stefania Chaplin

Solutions Engineer EMEA at Sonatype

schaplin@sonatype.com

@devopsbabe

sonatype.com/appscan

Sonatype

Get precise intelligence about the open source components used in your applications.

sonatype.com/appscan

sonatype.com/appscan

Sonatype