ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Edwin Kwan, Security Team Lead, Tyro

Keeping up with Open Source Security – An Automated, Developer Focused Approach

Talk Structure

- Open Source Security Matters
- Why Automated Developer Focused Approach
- Tyro's Open Source Security Journey
  - Automated time-based waivers
  - Security Self serve
- Next Steps

Open Source Security Matters


2019
State of the Software Supply Chain
The 5th annual report on global open source software development

Open Source is Everywhere

146B

Number of Java downloads in 2018

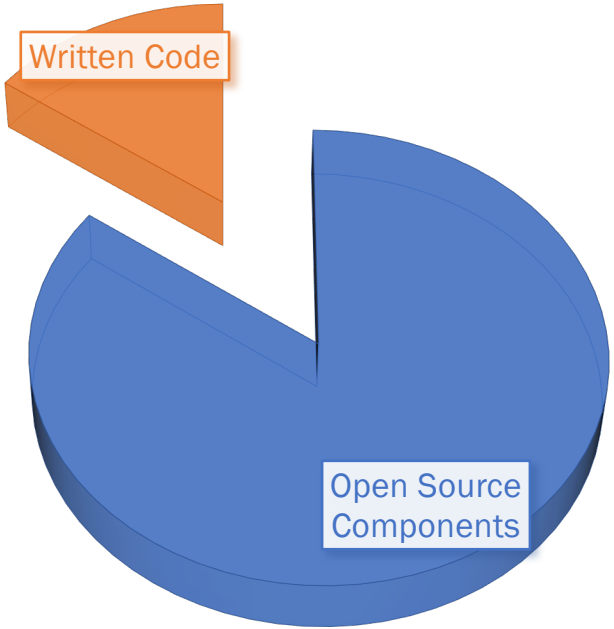
68%

Reference: State of Software Supply Chain Report

Open Source is Everywhere

85%

of modern applications
built from open source components



Reference: State of Software Supply Chain Report

Open Source are not built the same

10.3%

Percentage of downloaded vulnerable Java Components

Reference: State of Software Supply Chain Report

Open Source are not built the same

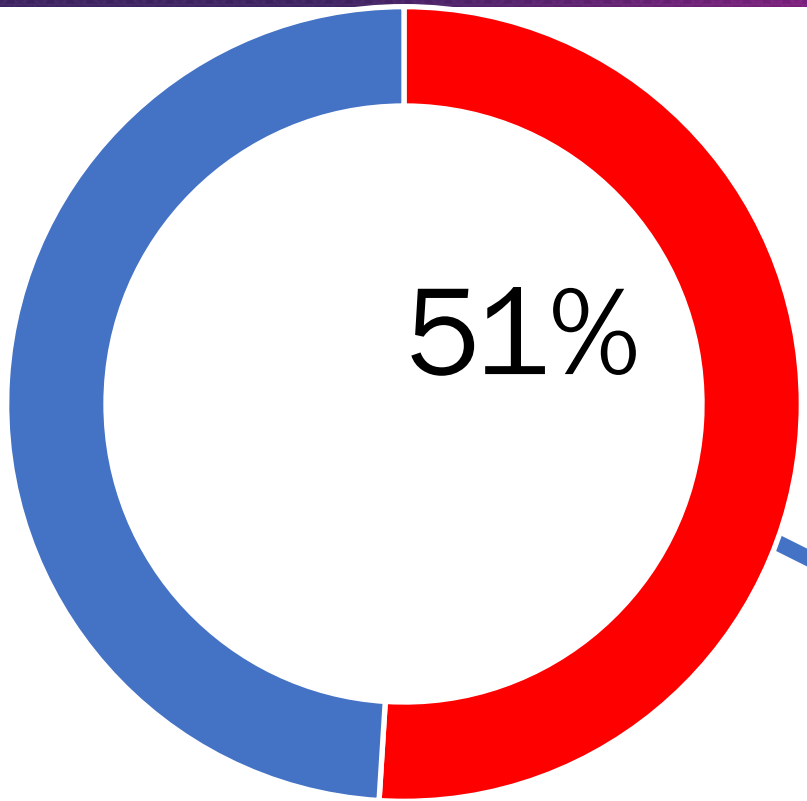
14,600,000,000

Number of downloaded vulnerable Java Components

Reference: State of Software Supply Chain Report

JS

Known vulnerabilities



1 in 3
rated high
Vulnerability.

1 in 10
Rated critical

Reference: State of Software Supply Chain Report

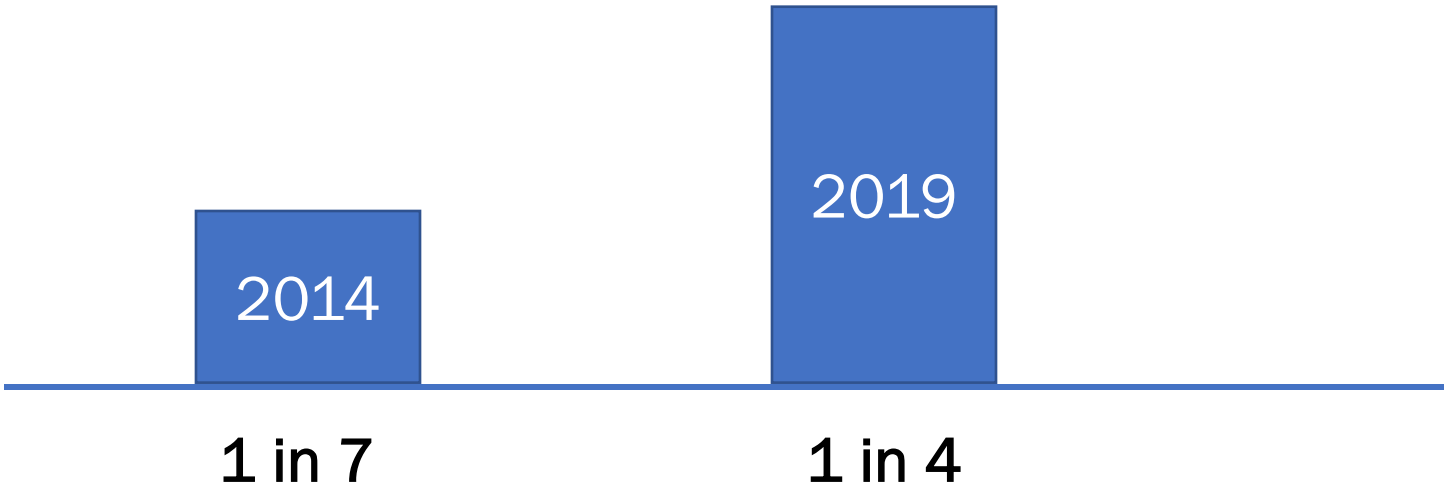
Increase Breaches

>70%

increase in breaches in open source components

DEVSECOPS
COMMUNITY
SURVEY 2019

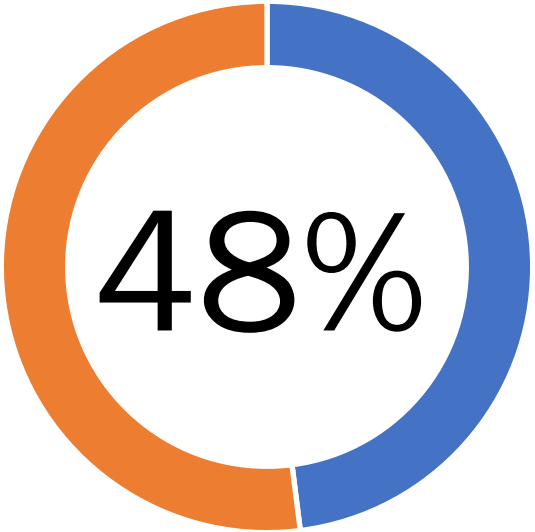
Increase Breaches



Reference: DevSecOps Community Survey

Why Automated Developer Focused Approach

Developers Care about Security



Developers continue to believe
security is important
but don't have enough time to spend on it

Reference: DevSecOps Community Survey

Top Challenges with AppSec

- We find out about problems too late in the process

- Slows down development

- Not clear what's expected of us

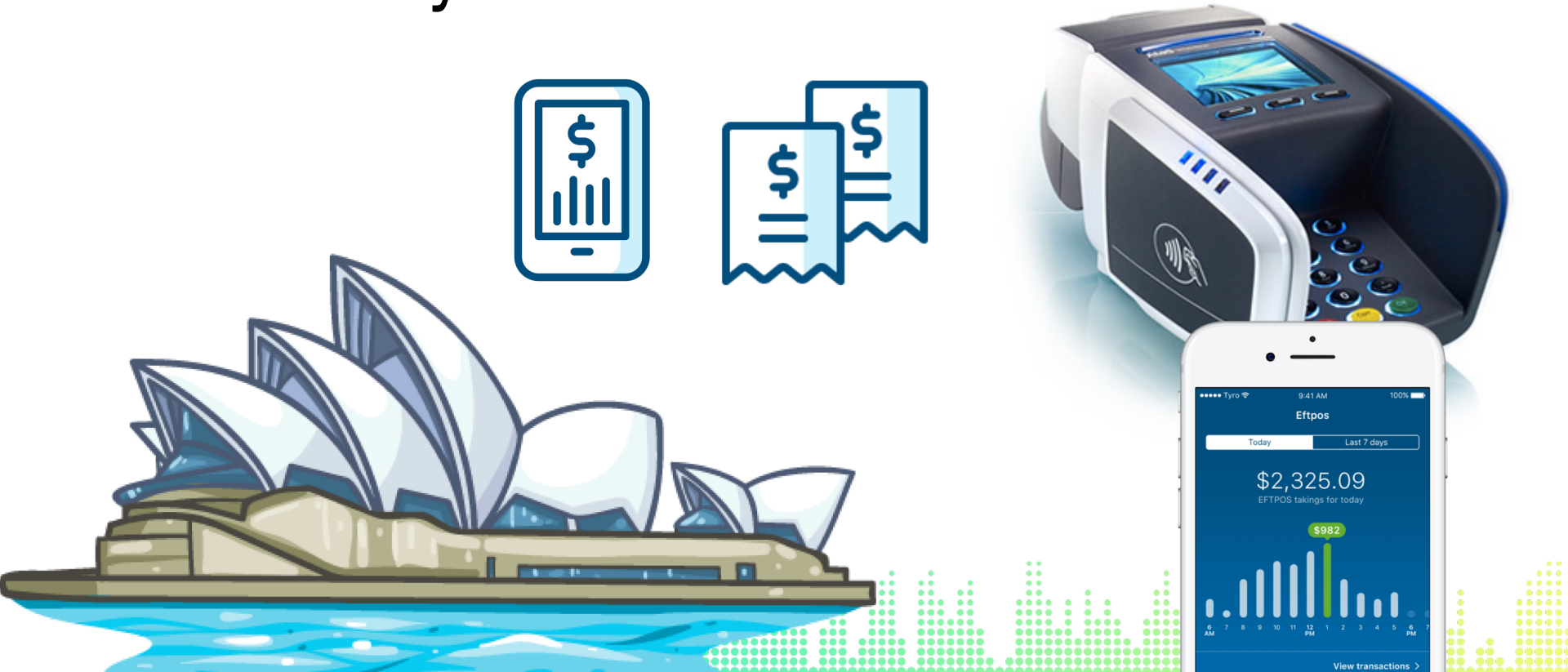
Reference: DevSecOps Community Survey

Tyro’s Open Source Security Journey

- Tyro’s Open Source Security Journey

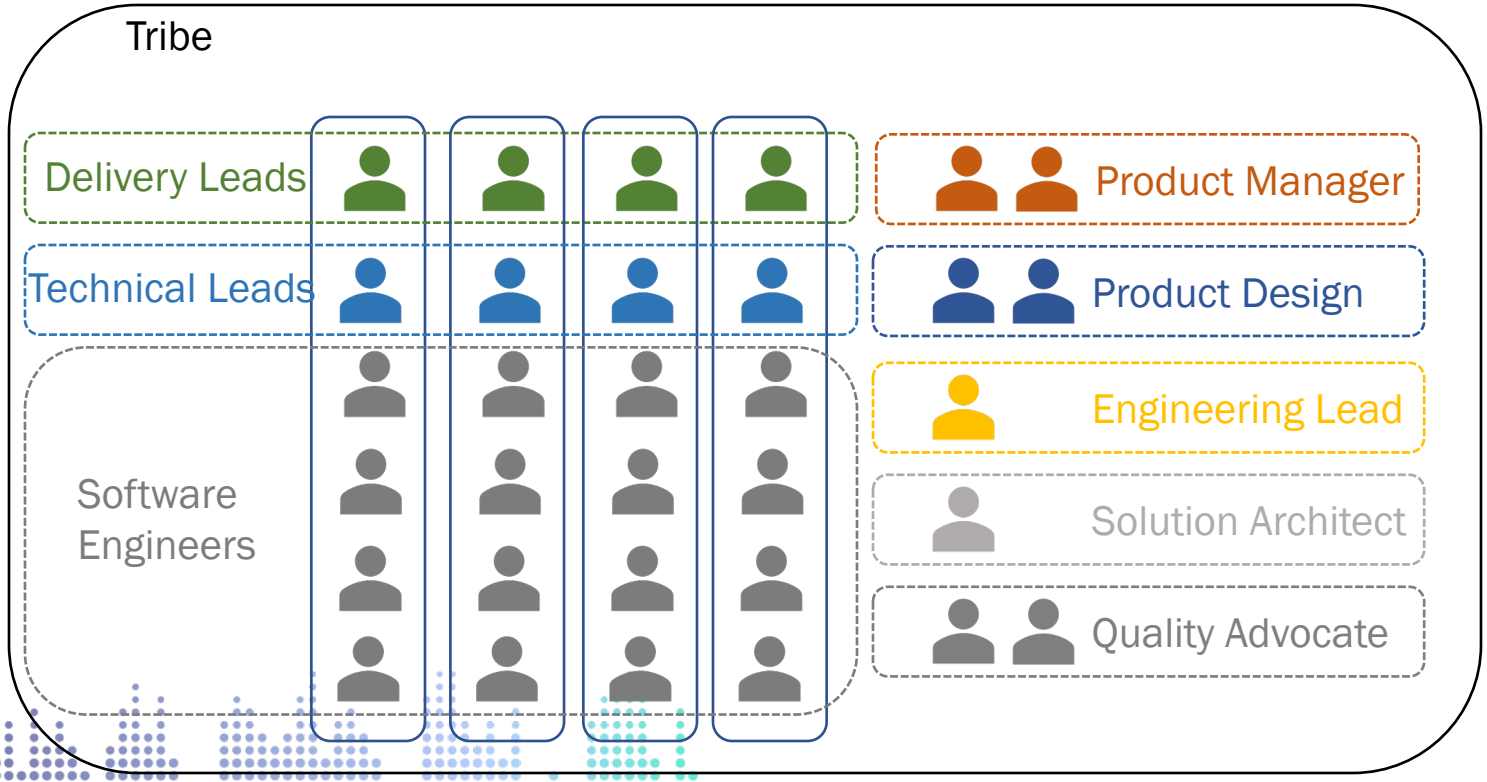
About Tyro

About Tyro

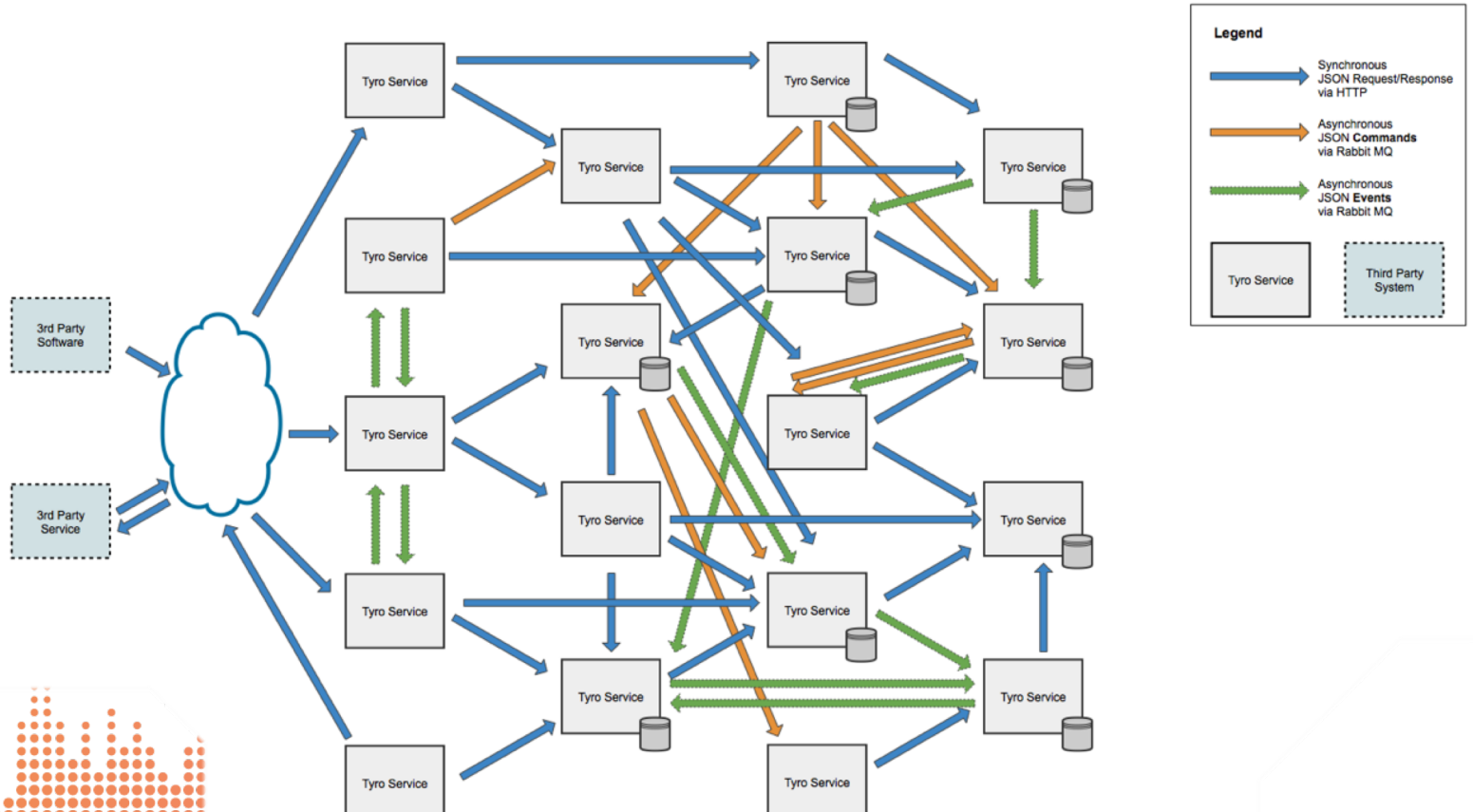

Tyro
9:41 AM
100%
Eftpos
Today
Last 7 days
$2,325.09
EFTPOS takings for today
$982
View transactions

About Tyro Engineering

Tyro Engineering



Micro-services Architecture

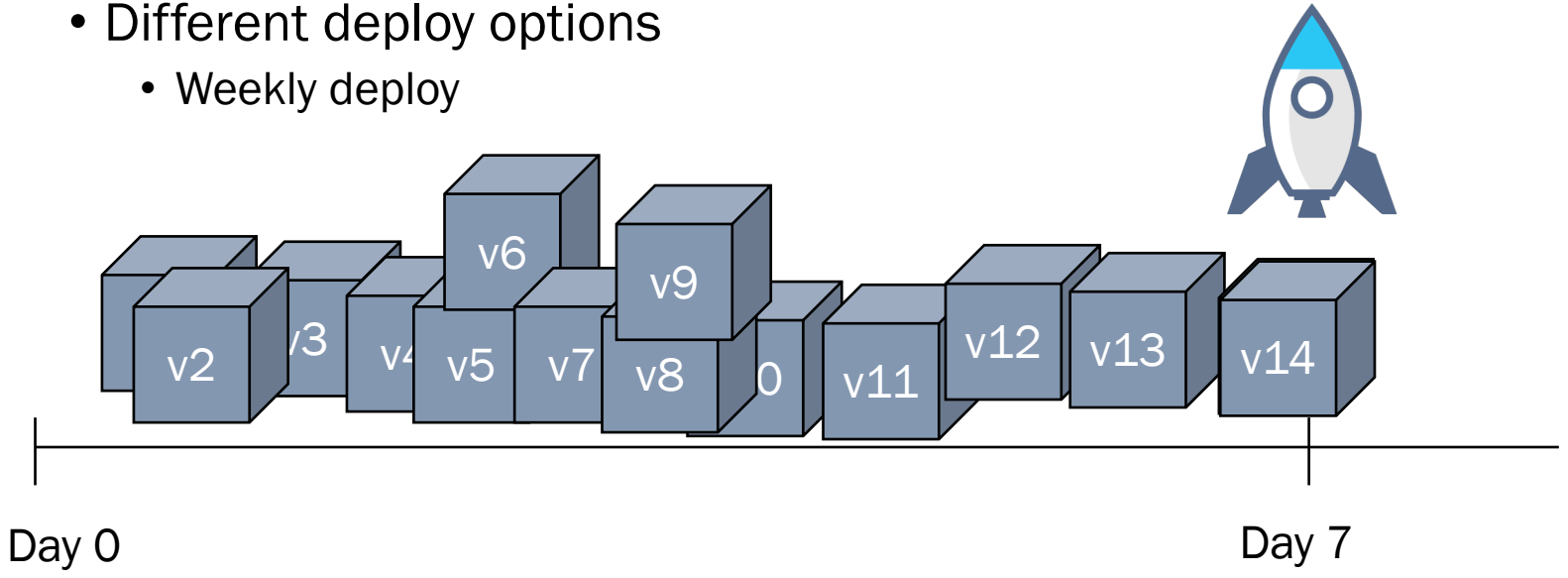


Continuous Release

- Different deploy options

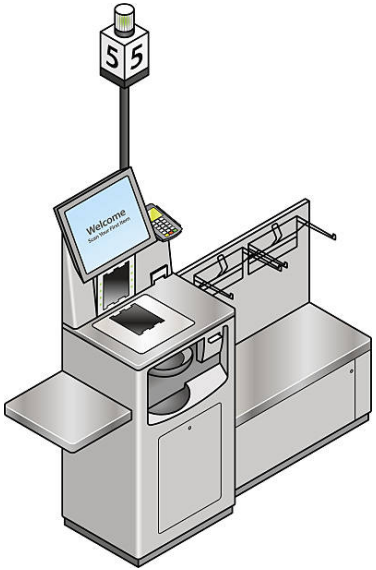
Continuous Release

- Different deploy options
  - Weekly deploy



Continuous Release

- Different deploy options
  - Weekly deploy
  - Self-serve deploy



Open Source Security Journey

Initial Open Source Scan

	6th September 2015
Critical	80
High	405
Medium	112
Low	-

From 63 Applications

Addressing CVEs

- Break build on security issues.

```
[INFO] ------------------------------------------------------------------------
[INFO] BUILD FAILURE
[INFO] ------------------------------------------------------------------------
[INFO] Total time: 4.329 s
[INFO] Finished at: 2018-01-25T11:25:56+11:00
[INFO] Final Memory: 38M/608M
[INFO] ------------------------------------------------------------------------
```

Addressing CVEs

- Break build on security issues.
- Grandfathered Existing CVEs.

Addressing CVEs

- Break build on security issues.
- Grandfathered Existing CVEs.
- Addressed CVEs based on priority.

Critical

High

Medium

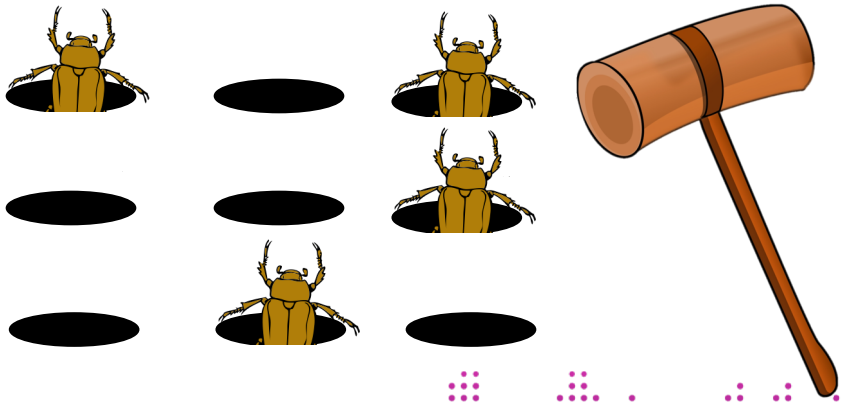
Low

Results

	6th September 2015	7th January 2016	21st July 2017
Critical	80	45	0
High	405	320	0
Medium	112	108	4
Low	-		2

Challenges

- Addressing Security issues is a continuous process.
- New issues are not grandfathered.



Automated Time-Based Waivers

SLA To Fix CVEs

Policy Severity	Grace Period (SLA)
Critical	fail immediately
High	4 weeks
Medium	3 months
Low	6 months

Automated Waivers

```
if ( CVE_discovery_date < SLA )
{
```

```
}else{
```

```
}
```

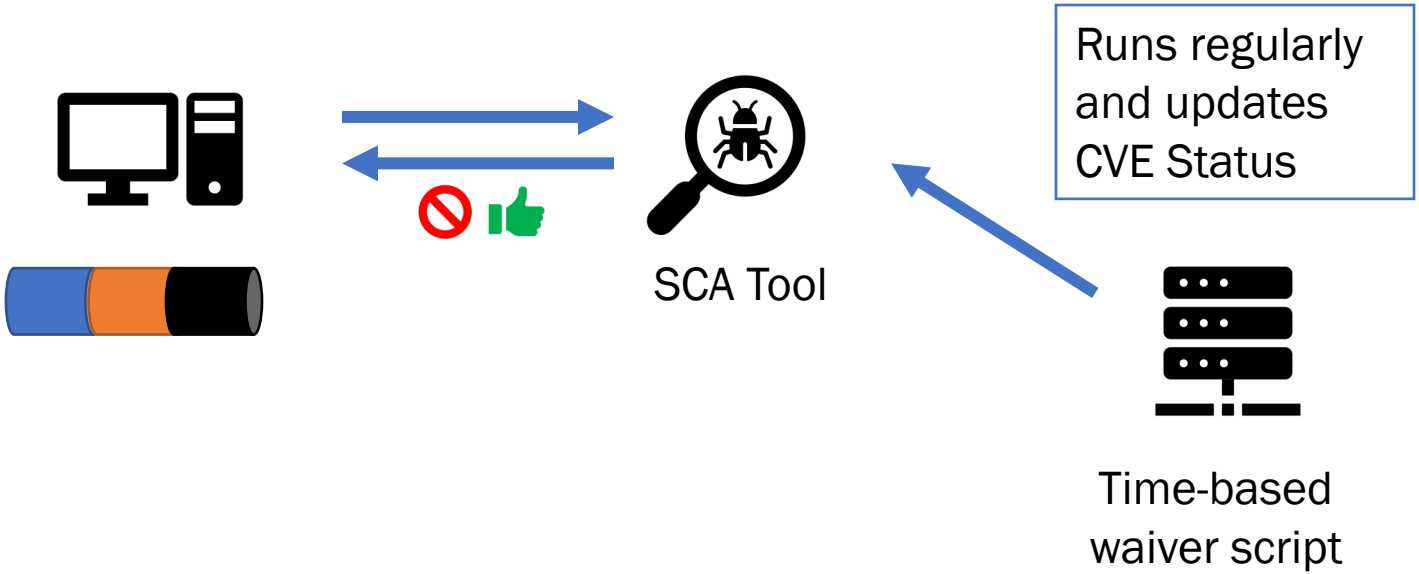
Implementation

- Two Security Policies for each severity

CVE status != Confirmed

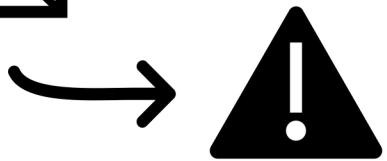
CVE == Confirmed

Implementation



Notification

- Email

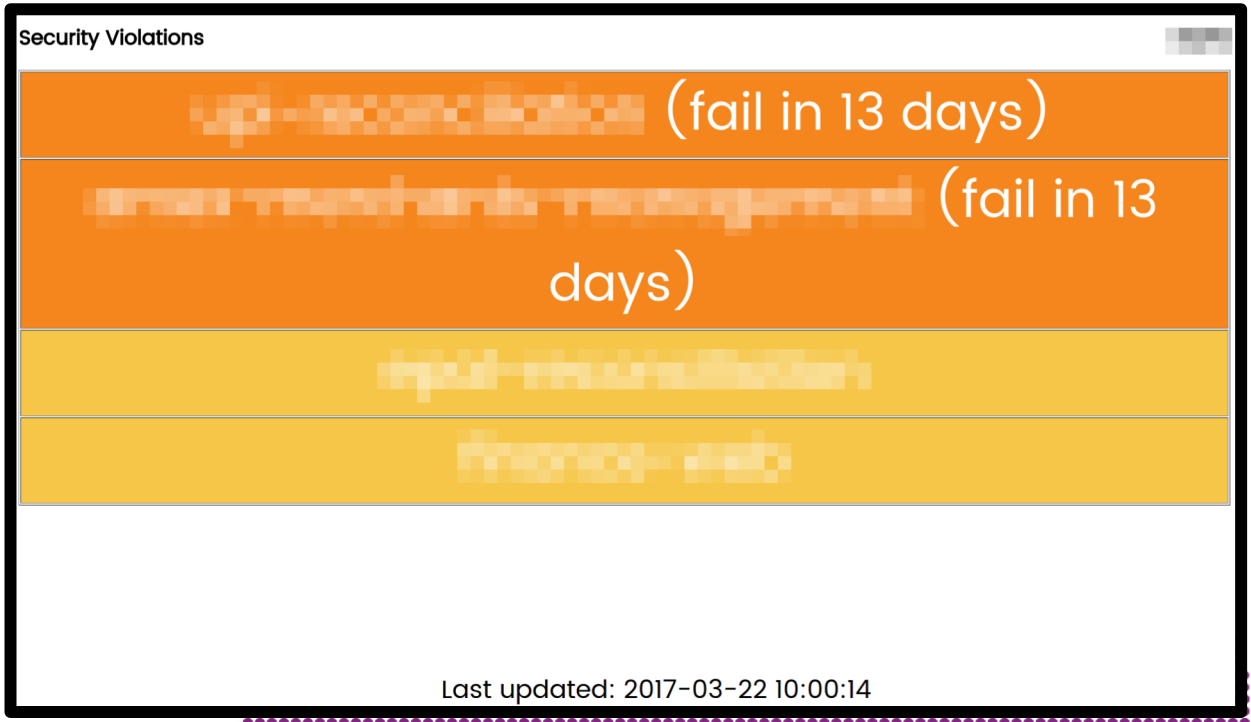


CVE Discovered in application abc

Please address by dd/mm/yyyy

Notification

- Email
- Dashboard



Notification

- Email
- Dashboard
- Confluence

Application	Component	Vul. Reference	Policy	Cur. Status	Next Non Vul. Ver.	Fixed by date
			SECURITY-MEDIUM	OPEN		(Due 82 days)
			SECURITY-LOW	OPEN	None	(Due 172 days)
		CVE-	SECURITY-MEDIUM	OPEN		(Due 82 days)

Resolution time periods based on

Policy	Resolution
SECURITY-CRTICAL	Immediate
SECURITY-HIGH	30 days
SECURITY-MEDIUM	90 days
SECURITY-LOW	180 days

CVE status Information:

Below is information on different vulnera

Actionable Intelligence

- Automatically extend waivers for issues when there are no fix available.

Security Self Serve

Security Self Serve

- Allows teams to apply for an extension for security issues whose SLAs have expired.
- Allows builds to be passing again.

Why Security Self Serve

- Business priorities.
- Require more time to address.

Security Self Serve

Requires Technical Lead Approval

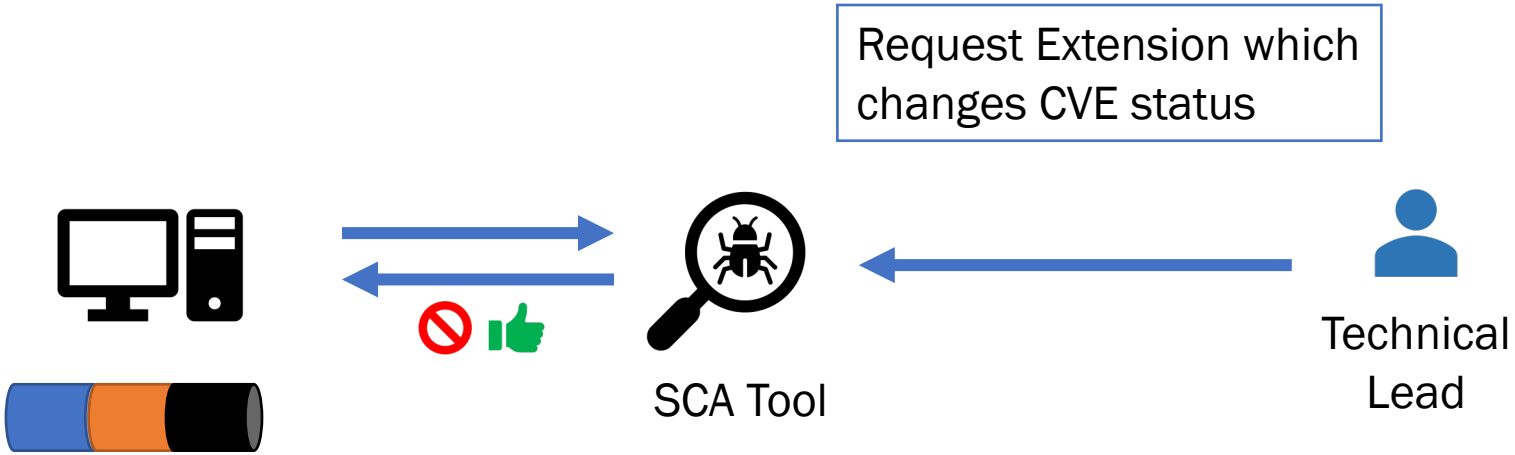
14

days

Extension Time

Regularly Reviewed

Security Self Serve

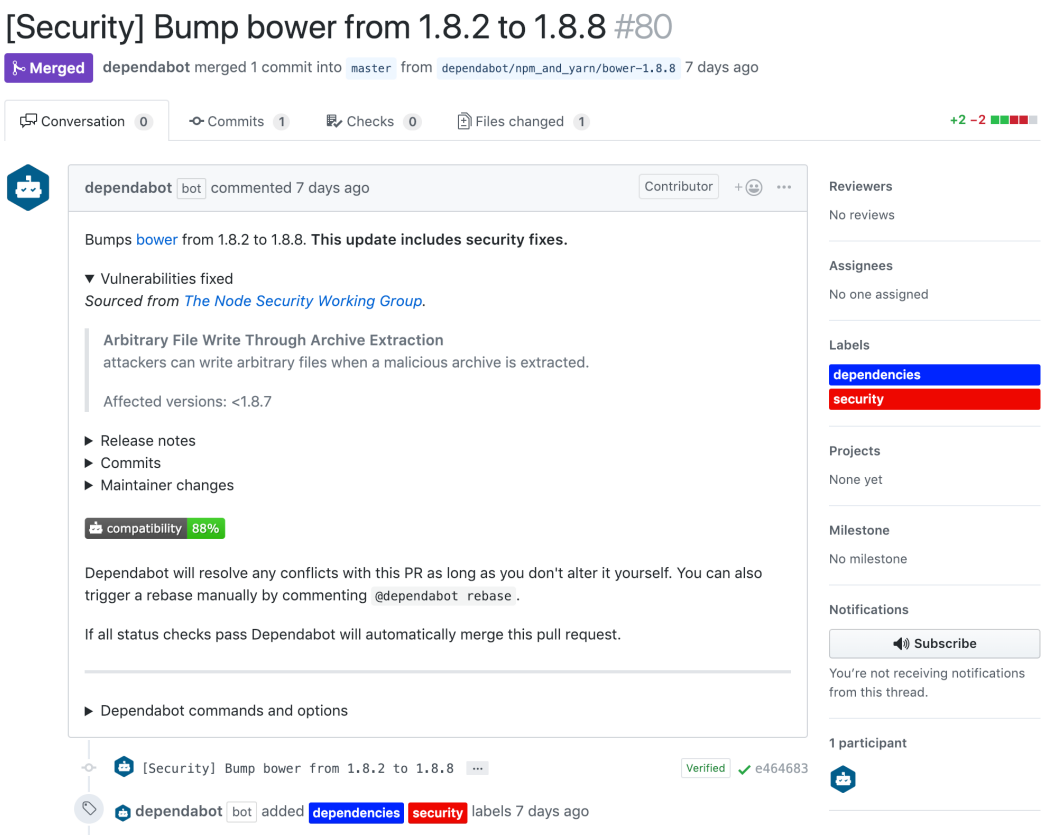


Security Self Serve

Reverts CVE status to Confirmed after 14 days

Next Steps

Shifting Further Left



[Security] Bump bower from 1.8.2 to 1.8.8 #80

Merged dependabot merged 1 commit into master from dependabot/npm_and_yarn/bower-1.8.8 7 days ago

Conversation 0 · Commits 1 · Checks 0 · Files changed 1 · +2 −2

dependabot bot commented 7 days ago — Contributor

Bumps bower from 1.8.2 to 1.8.8. **This update includes security fixes.**

▼ Vulnerabilities fixed
Sourced from The Node Security Working Group.

> **Arbitrary File Write Through Archive Extraction**
> attackers can write arbitrary files when a malicious archive is extracted.
>
> Affected versions: <1.8.7

▶ Release notes
▶ Commits
▶ Maintainer changes

compatibility 88%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

If all status checks pass Dependabot will automatically merge this pull request.

▶ Dependabot commands and options

[Security] Bump bower from 1.8.2 to 1.8.8 ··· Verified e464683

dependabot bot added dependencies security labels 7 days ago

Reviewers
No reviews

Assignees
No one assigned

Labels
dependencies
security

Projects
None yet

Milestone
No milestone

Notifications
Subscribe
You're not receiving notifications from this thread.

1 participant

Conclusion

Lessons Learned

- Open Source Security Matters
- It should be automated
- It should empower developers

ADDO
ALL DAY DEVOPS

SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

GOLD SPONSORS

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

MEDIA SPONSORS