Microsoft

Who Wants a Thousand Free Puppies?

Michael Scovetta
Principal Security PM Manager
Microsoft

LocoMocoSec 2019

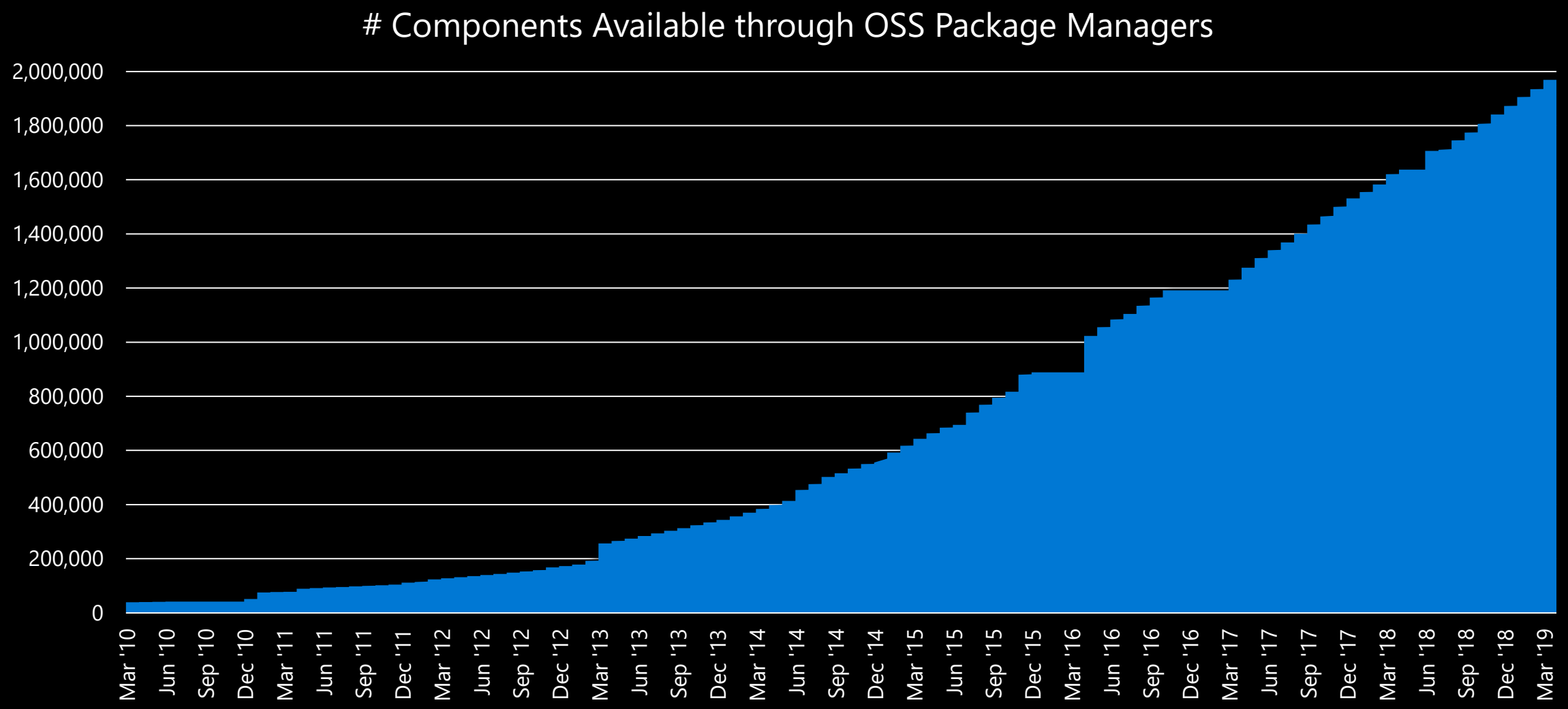
Image Source: https://pixabay.com/photos/hawaii-oahu-waterfall-rocks-1034890/

April 2014

Source: https://upload.wikimedia.org/wikipedia/commons/thumb/d/dc/Heartbleed.svg/2000px-Heartbleed.svg.png

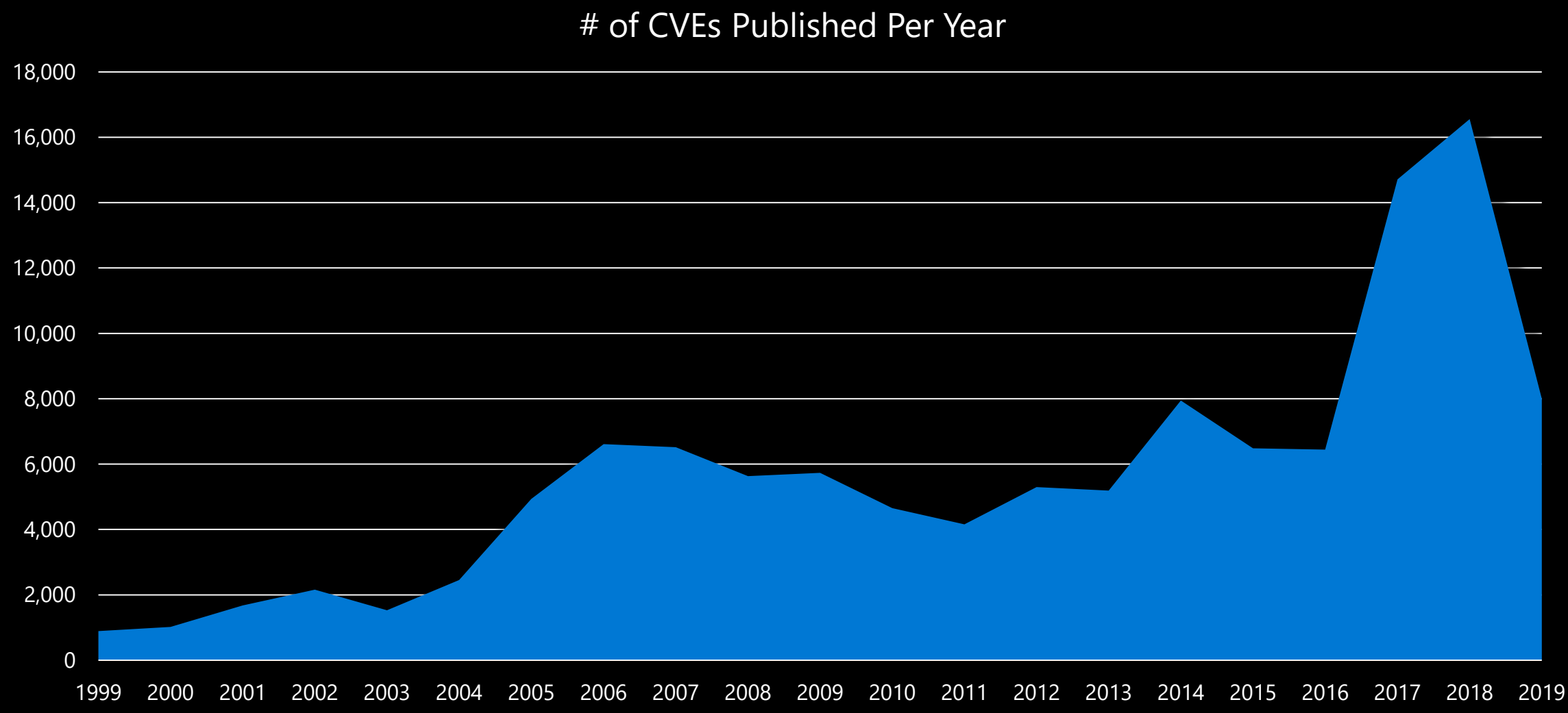
Open Source can be a little bit scary.

Increasing Volume of OSS Available…



Data courtesy of modulecounts.com

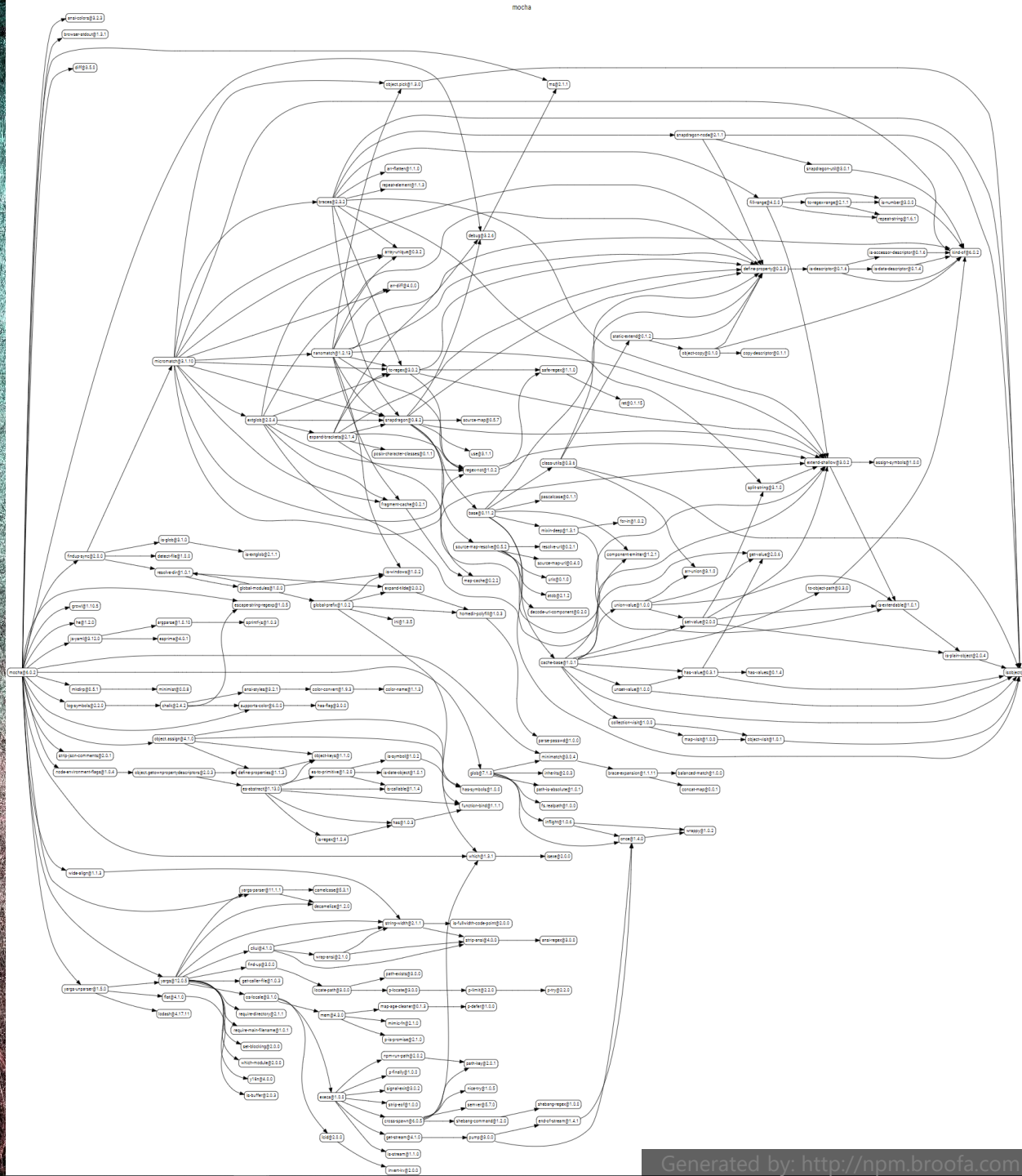
High Volume of Vulnerabilities…



Data courtesy of cvedetails.com

Increasing Complexity...

Increasing Complexity...



Your company is responsible for
everything that ships.

Because an attacker doesn't care
who wrote a piece of vulnerable software.

Neither will your customers when you have to notify them of a breach.

How does Microsoft manage security risk related to our use of open source software?

Four "Simple" Tasks

1	Identify What OSS is Used
2	Centrally Catalog Identified OSS
3	Ensure the OSS is Secure
4	Respond to Security Vulnerabilities

Task #1: Identify What OSS is Used

Modern software is often built by combining many pre-existing components in novel ways, which drives increased use of OSS.

As a first step, we must understand what OSS is being used so that we can properly manage it.

This “discovery” process requires high-quality automation. Without that, software developers have the difficult, error-prone, and time-consuming task of trying to identify OSS manually.

Task #1: Identify What OSS is Used *(continued)*

What does this “discovery” look like?

A software program is scanned by a “discovery” tool, which looks for traces of OSS components, each of which is identified and emitted into a report. Often referred to as a bill of materials.

Task #2: Centrally Catalog Identified OSS

All identified OSS must be available through efficient tooling (such as a central database).

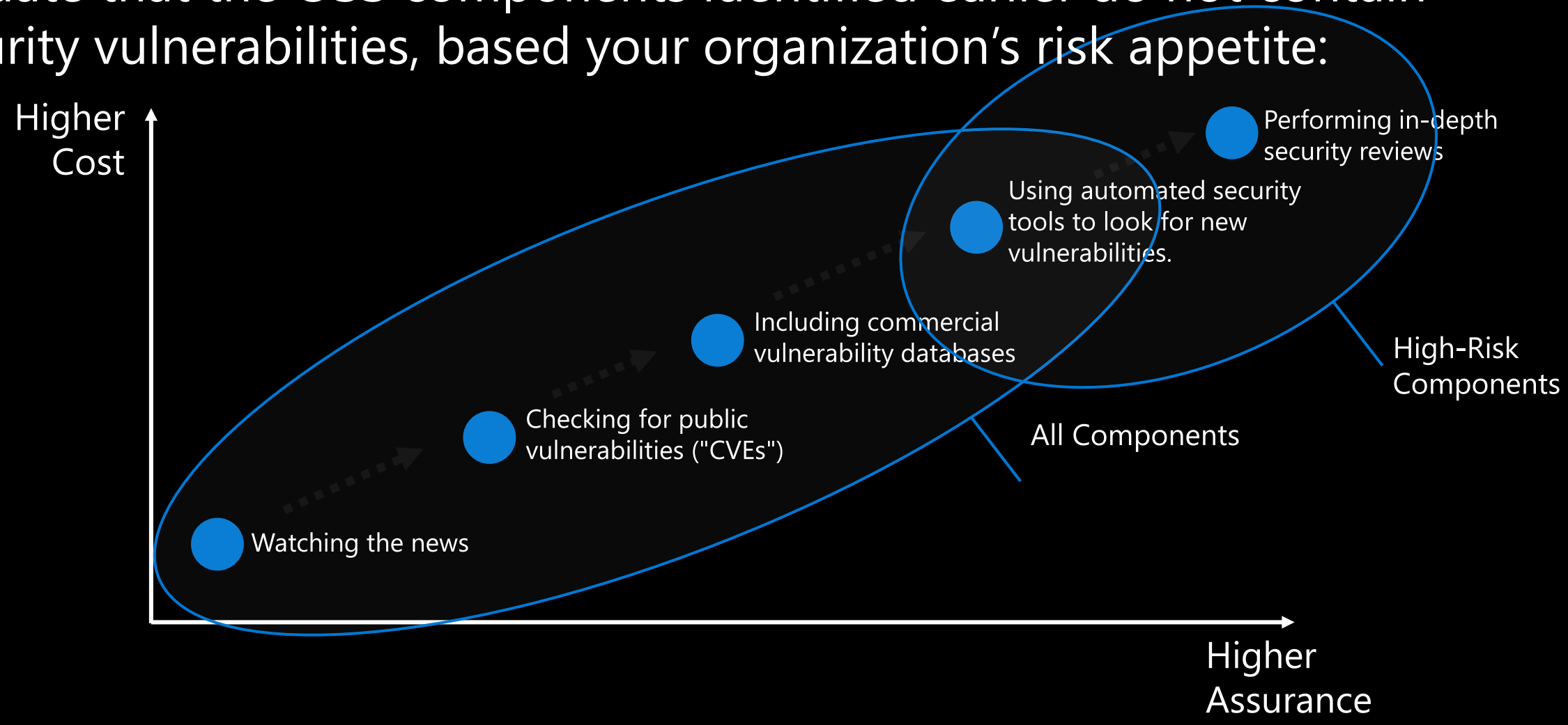
This enables the following:

- Improved understanding of an organization's use of OSS.
- Increased response time, decreased cost:
  - *Which software products would be affected by a vulnerability in a particular OSS component?*

Since component usage evolves over time, also lets you identify for how long a potentially vulnerable component was used.

Task #3: Ensure the OSS is Secure

Validate that the OSS components identified earlier do not contain security vulnerabilities, based your organization's risk appetite:

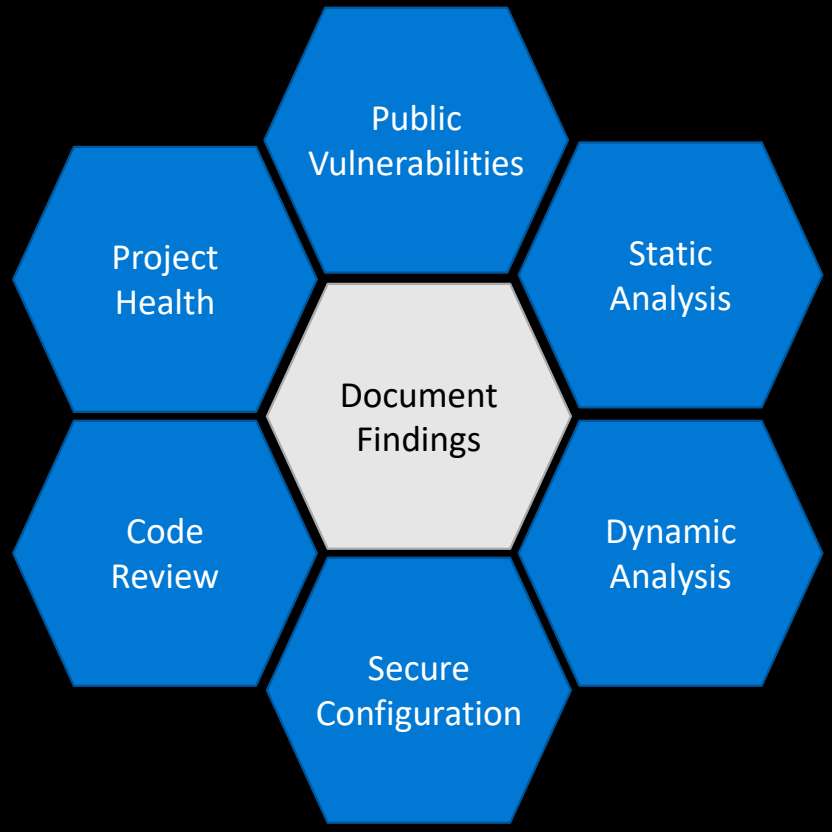


Task #3: Ensure the OSS is Secure *(continued)*

In-Depth Security Reviews

Can be expensive, but offers a high assurance that components meet security requirements.

At Microsoft, we have a dedicated team performing this function, augmented by engineering teams themselves.



Open Source Security Unified Metabase

Search

Left-Pad 1.3.0 | String left pad

Component Information

Basic information about this component

GitHub metadata is not available at this time.

URLs associated with this project include:

- github.com/stevemao/left-pad
- github.com/camwest/left-pad
- github.com/azer/left-pad

Component Health

Is the component still being maintained?

Notes

Overall Component Health	Good
Still Maintained?	Poor
Responds to Issues?	Good
Responds to Security Issues?	Poor
Responds to Pull Requests?	Great

Updated 17 hours, 52 minutes ago. Refresh

Details...

Release

What is the latest release of this component?

Download

Great! This is the latest version of this component.

Versions released per year

Last updated 2 weeks ago.

Reviews

Reviews for this component

Title	Type	Approval	Published
Security Review	Security	✓	Apr 2019
Reviews for other versions:			
Security Review	Security	ℹ	Mar 2017
Security Review	Security	ℹ	Mar 2017

Typosquatted packages

Packages that are similar in spelling to this component

left-sad leftpad left_pad reft-pad

Dependencies

What components does this depend on?

This component does not have any known dependencies.

Last updated 2 weeks ago.

Related Components

Find components similar to this one

Sorry, no components were found similar to this one.

Attributes

What does this component do?

Categories

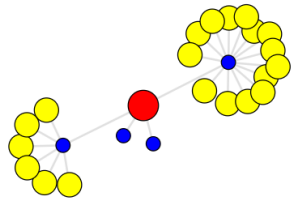
Sorry, no categories were found.

Tags

leftpad left pad padding string repeat

Maintainers

Who contributes to this component?
What other components do they contribute to?



This is an internal tool we use to manage security data for OSS components.

Open Source Security Unified Metabase

Search

Left-Pad 1.3.0 | String left pad

Component Information

Basic information about this component

GitHub metadata is not available at this time.

URLs associated with this project include:

- github.com/stevemao/left-pad
- github.com/camwest/left-pad
- github.com/azer/left-pad

Component Health

Is the component still being maintained?

Notes

Overall Component Health	Good
Still Maintained?	Poor
Responds to Issues?	Good
Responds to Security Issues?	Poor
Responds to Pull Requests?	Great

Updated 17 hours, 52 minutes ago. Refresh

Details...

Release

What is the latest release of this component?

Download

Great! This is the latest version of this component.

Versions released per year

2016 2017 2018

Reviews

Reviews for this component

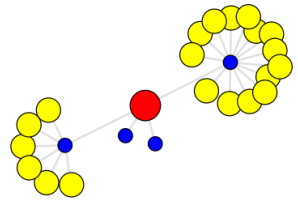
Title	Type	App
Security Review	Security	
Reviews for other versions:		
Security Review	Security	
Security Review	Security	

Related Components

Find components similar to this one

Sorry, no components were found similar to this one.

leftpad left pad padding string repeat



This is an internal tool we use to manage security data for OSS components.

Open Source Security Unified Metabase

Search

Left-Pad 1.3.0 | String left pad

Component Information

Basic information about this component

GitHub metadata is not available at this time.

URLs associated with this project include:

- github.com/stevemao/left-pad
- github.com/camwest/left-pad
- github.com/azer/left-pad

Component Health

Is the component still being maintained?

Notes

Overall Component Health	Good
Still Maintained?	Poor
Responds to Issues?	Good

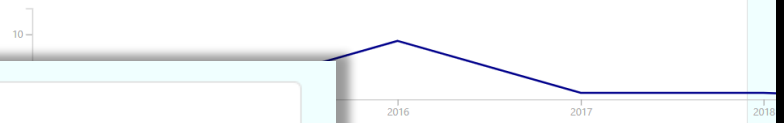
Release

What is the latest release of this component?

Download

Great! This is the latest version of this component.

Versions released per year



Typosquatted packages

Packages that are similar in spelling to this component

left-sad leftpad left_pad reft-pad

Reviews

Reviews for this component

Title	Type
Security Review	Security
Reviews for other versions:	
Security Review	Security
Security Review	Security

Related Components

Find components similar to this one

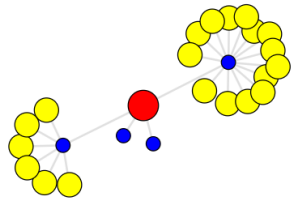
Sorry, no components were found similar to this one.

Categories

Sorry, no categories were found.

Tags

leftpad left pad padding string repeat



This is an internal tool we use to manage security data for OSS components.

Open Source Security Unified Metabase

Search

Left-Pad 1.3.0 | String left pad

Component Information

Basic information about this component

GitHub metadata is not available at this time.

URLs associated with this project include:

- github.com/stevemao/left-pad
- github.com/camwest/left-pad
- github.com/azer/left-pad

Component Health

Is the component still being maintained?

Notes

Overall Component Health	Good
Still Maintained?	Poor

Release

What is the latest release of this component?

Download

Great! This is the latest version of this component.

Versions released per year

Reviews

Reviews for this component

Title	Type	Approval
Security Review	Security	
Reviews for other versions:		
Security Review	Security	
Security Review	Security	

Related Components

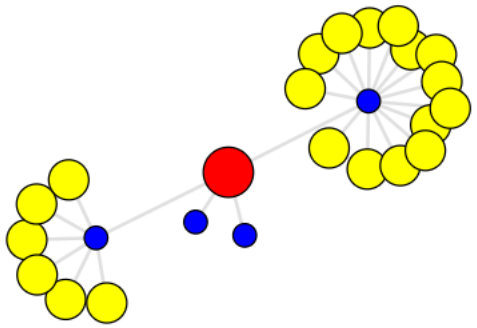
Find components similar to this one

Sorry, no components were found similar to this one.

Maintainers

Who contributes to this component?

What other components do they contribute to?

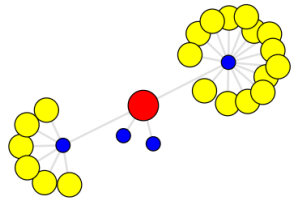


depend on?

any known dependencies.

onent?

hey contribute to?



Tags

leftpad left pad padding string repeat

This is an internal tool we use to manage security data for OSS components.

Task #3: Ensure the OSS is Secure *(continued)*

Flagging a Component as Vulnerable

Multiple sources of vulnerability data:

- Public data (e.g. CVEs)
- Commercial / Curated data
- Security assessments
- Static analysis results

- Engineers are automatically notified of new vulnerabilities.

- Advice is often to simply upgrade to the latest (stable) version.

Task #4: Respond to Security Vulnerabilities

Integrate OSS security response into your organization's security response program.

At Microsoft, our response process is managed by the Microsoft Security Response Center (MSRC).

Key difference for OSS – limited understanding of external parties:

- Are they trustworthy?
- Are they competent?
- Will they fix the OSS component?
- Will they respond at all?
- How should we respond if a fix won't be made available by the author? Fork? Announce?

Four "Simple" Tasks

- ✓ Identify What OSS is Used
- ✓ Centrally Catalog Identified OSS
- ✓ Ensure the OSS is Secure
- ✓ Respond to Security Vulnerabilities

What else should we be thinking about?

Build from Source
How do you know the binaries "match" the source?

Typo-Squatting
Did you mean "crossenv" or "cross-env"?

High-Risk Components
How to identify these? What additional vetting should you do?

Blessed Package Repository
Is your CI infrastructure pulling packages from the Internet?

Freshness
Keep your OSS up to date, even without known vulnerabilities.

Program Management
Do you have a coherent, managed OSS security program?

July 12, 2018

The Register®
Biting the hand that feeds IT

Security

Now Pushing Malware: NPM package dev logins slurped by hacked tool popular with coders

Tokens killed after eslint-scope utility compromised

By Shaun Nichols in San Francisco 12 Jul 2018 at 20:13 9 SHARE ▼

Updated An unfortunate chain reaction was averted today after miscreants tampered with a widely used JavaScript programming tool to steal other developers' NPM login tokens.

Source: https://www.theregister.co.uk/2018/07/12/npm_eslint/

Are there any more out there?

How many more are out there?

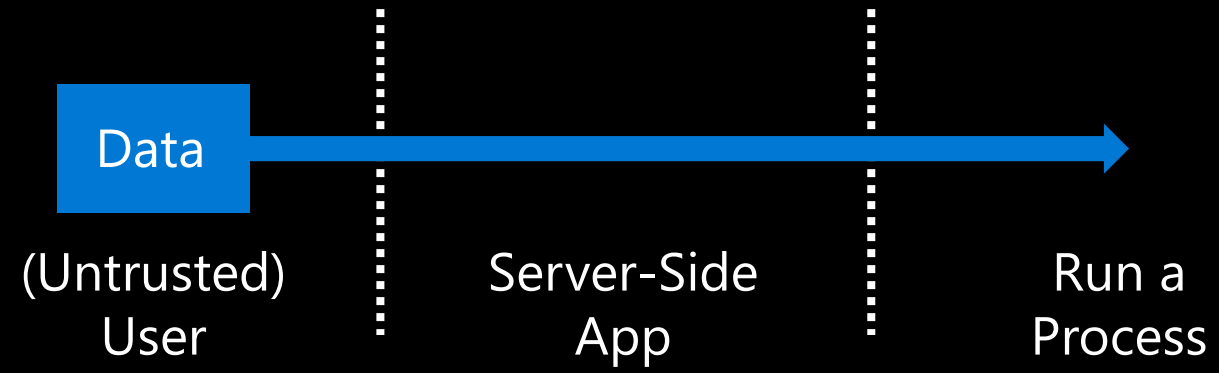
Experiment

Hypothesis:

We can efficiently detect patterns like those used in the eslint-scope.

Methodology:

We wrote a custom static analysis rule and ran it against randomly sampled NPM projects, looking for the following pattern:



> We look for data coming from the remote user (HTTP GET/POST parameter) and flowing to `child_process.exec`.

Results

Components Scanned

50,000

Identified Vulnerabilities

14

Confirmed Vulnerabilities

14

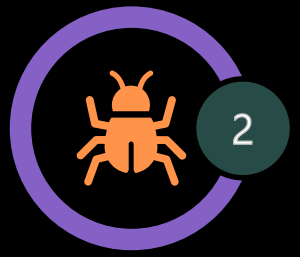
None of the identified vulnerabilities appeared to be malicious. Rather, they looked like an accidental security bug.

MSRC

Key Takeaways & Learnings

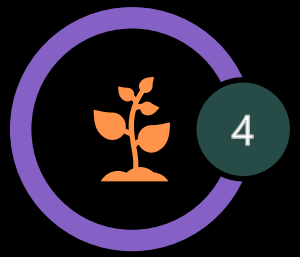
Wherever you are on your journey, remember these key ideas when managing your open source security program.

Keep an accurate inventory of the open source you use.



Use high-quality vulnerability data sources (not only CVEs).

Leverage your existing incident management processes to respond to OSS vulnerabilities.



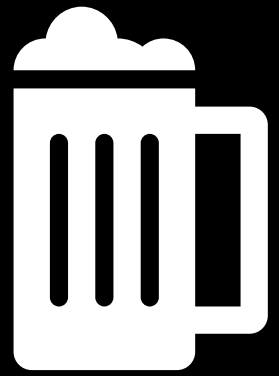
It's often better to update a vulnerable component than determine if you're vulnerable.

Keep a closer eye on the high-risk OSS you're using.

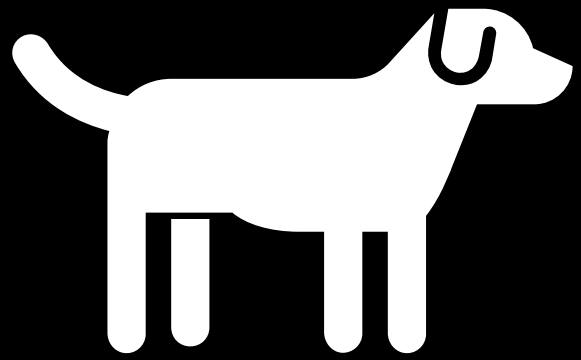
Encourage developers to adopt practices that keep OSS components up to date.

Stay on top of the fast-moving OSS ecosystem.

Some people think open source is free as in free beer.



It's actually more like a free as in a free puppy.



Thank You!