THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
EUROPE

Securing open-source

Dependencies, incident response, vulnerabilities, and bug bounties

Maya Kaczorowski
Product Manager, Google Cloud

October 28, 2019

THE LINUX FOUNDATION

What’s a Birds of a Feather (BoF) talk?

Informal meeting

Group based on common interests

Discussion-based

- Questions
- Comments
- Examples

Who am I?

Maya Kaczorowski

Product Manager,
Container Security

Google Cloud

@MayaKaczorowski

Discussion topic: Securing open-source

- Dependencies
- Vulnerability management
- Incident management
- Bug bounties

Dependencies

Your open-source project has dependencies on other projects

How do you manage dependencies?

- Whose responsibility is it to update dependencies?
- How do you vet your dependencies?
- How do you update dependencies?
- How do you remove dependencies that are no longer needed?

Dependencies
Case study: distroless images

Kubernetes is rebasing its main master and node images to distroless

Distroless images are images with minimal language-focused packages only

- **Minimal**: Only your application and its runtime dependencies - no package managers or shells
- **Many languages**: java, python, Node.js, .NET, etc.

https://github.com/kubernetes/enhancements/blob/master/keps/sig-release/20190316-rebase-images-to-distroless.md

Vulnerability management

Your open-source project's dependencies have vulnerabilities

How do you find and patch vulnerabilities?

- How do you scan for vulnerabilities?
- Whose responsibility is it to patch vulnerabilities?

Incident management

Your project will find vulnerabilities for which you need to distribute a fix

How do you respond to new security issues and incidents?

- How do you search for vulnerabilities?
- How does a researcher alert you of an issue they found?
- How do you triage a potential issue?
- Who has the ability to fix the issue?
- How do you fix and address the issue privately?
- How do you deal with ‘security releases’?

Incident management

Case study: Kubernetes security audit

Kubernetes completed a security audit in August 2019

- Funded by the CNCF
- In collaboration with security experts on Kubernetes
- Publicly published results, tracking resolution publicly

https://www.cncf.io/blog/2019/08/06/open-sourcing-the-kubernetes-security-audit/

https://github.com/kubernetes/kubernetes/issues/81146

Incident management

Case study: Kubernetes Product Security Committee

- Report a vulnerability at security@kubernetes.io
- Clear guidelines on communications and public disclosure timelines
- Fix development process to triage, get expertise, obtain CVE if needed, develop fix in private, and cut a release
- Fix disclosure process for private distributors' list and public at kubernetes-security-announce@googlegroups.com

https://kubernetes.io/docs/reference/issues-security/security/
https://github.com/kubernetes/security/blob/master/security-release-process.md
https://cloud.google.com/blog/products/containers-kubernetes/exploring-container-security-vulnerability-management-in-open-source-kubernetes

Bug bounties

Your open-source project may want to reward and incentivize researchers who discover vulnerabilities

How do you manage a bug bounty program?

- Should you even have a bug bounty program?
- Will this increase real, useful research?
- Who will do first line triage?
- Who will pay rewards?

Bug bounties
Case study: Internet Bug Bounty

The Internet Bug Bounty covers a range of large open-source projects: Python, Ruby, PHP, Django, Perl, nginx, OpenSSL, etc.

- Sponsored by Facebook, GitHub, Ford Foundation, Microsoft and HackerOne
- Bugs reviewed by a cross-company panel
- Rewarded $730K+ in bounties to 199 researchers for 817 flaws, including: ImageTragick, Heartbleed, and Shellshock

https://internetbugbounty.org/

What you can do today

- Create a security reporting email address or group
- Add a security policy file SECURITY.md with information on how to report security issues
- Try out your process

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

EUROPE