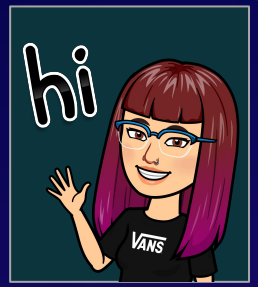
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Simplifying coordinating vulnerabilities & disclosures in open source projects

OSS-NA 2023

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



Madison Oliver, @taladrane

Pronunciation: TALA-drane

Security transparency & disclosure advocate

Cat fancier & WoW enthusiast

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

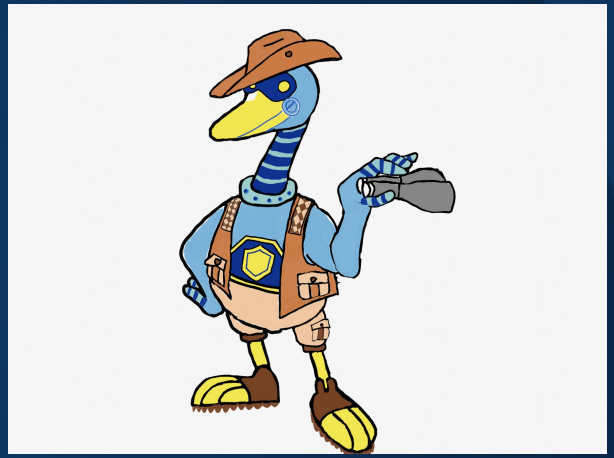
42nd level Dungeon Master

25th level Securityologist

Pirate-enthusiast & hat-owner

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Agenda



01

Key Vulnerability handling concepts & terms

02

Why CVD is important?

03

How to do CVD?

04

What makes CVD hard?

05

How can YOU help?

Some concepts to help our conversation...

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Coordinated Vulnerability Disclosure (CVD)

The process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public.

Principles of CVD

- Reduce Harm
- Presume Benevolence
- Avoid Surprise
- Incentivize Desired Behavior
- Ethical Considerations
- Process Improvement

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Embargo

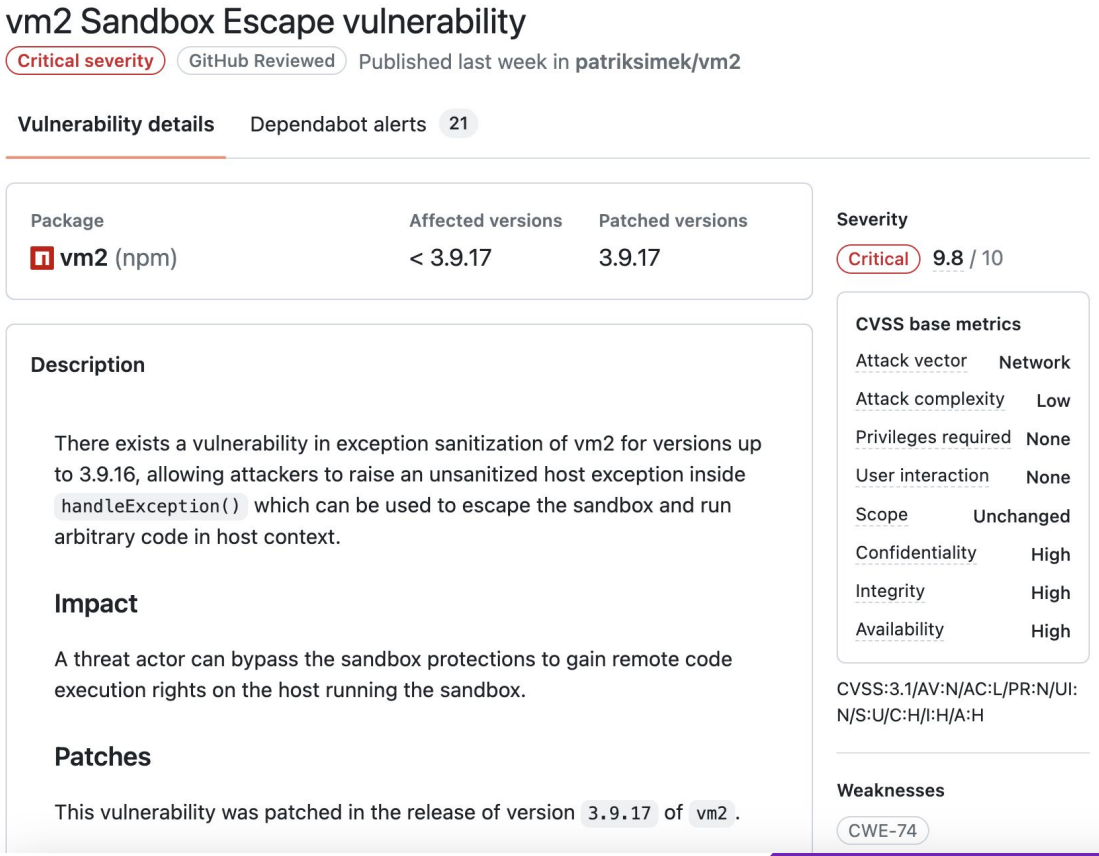
A hold on the publication of vulnerability details until affected parties are able to release security updates or mitigations and workarounds to protect downstream.

https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1#Definitions

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

(Security) Advisory

An announcement or bulletin that serves to inform, advise, and warn about a vulnerability within a component.



vm2 Sandbox Escape vulnerability

Critical severity | GitHub Reviewed | Published last week in **patriksimek/vm2**

Vulnerability details | Dependabot alerts 21

Package	Affected versions	Patched versions
vm2 (npm)	< 3.9.17	3.9.17

Description

There exists a vulnerability in exception sanitization of vm2 for versions up to 3.9.16, allowing attackers to raise an unsanitized host exception inside `handleException()` which can be used to escape the sandbox and run arbitrary code in host context.

Impact

A threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox.

Patches

This vulnerability was patched in the release of version `3.9.17` of `vm2`.

Severity

Critical 9.8 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Weaknesses

CWE-74

https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1#Definitions

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

CSAF

Common Security Advisory Framework - A language to exchange Security Advisories. The "next generation" of the earlier Common Vulnerability Reporting Framework (CVRF) standard.

https://oasis-open.github.io/csaf-documentation/

VEX

Vulnerability Exploitability eXchange - A document or statement that allows a software supplier or other parties to assert the status of specific vulnerabilities in a particular product.

https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Document_508c.pdf

Vulnerability Disclosure Program (VDP)

A structured process for reporting vulnerabilities. It often includes a disclosure policy that gives clear guidelines on:

- How and where 3rd parties can notify the VDP of a security vulnerability
- How to conduct good faith research
- The process that the 3rd party can expect (typically timeframes)
- How the report will be evaluated

https://docs.hackerone.com/organizations/vdp-vs-bbp.html

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Bug Bounty Program (BBP)

Incentivizes external third parties to find security vulnerabilities in a company's software and report them directly to the company so they can be safely resolved.

- Finders of the vulnerabilities are rewarded with monetary prizes.
- BBPs have the option to be *private* or *public*.
- A BBP can be a part of your vulnerability disclosure program (VDP).

https://docs.hackerone.com/organizations/vdp-vs-bbp.html
https://bugbountycoi.org/

Safe Harbor

A provision that offers protection from liability in certain situations, usually when certain conditions are met.

- Common in copyright law (like the Digital Millennium Copyright Act (DMCA))

In the context of *security research and vulnerability disclosure*…

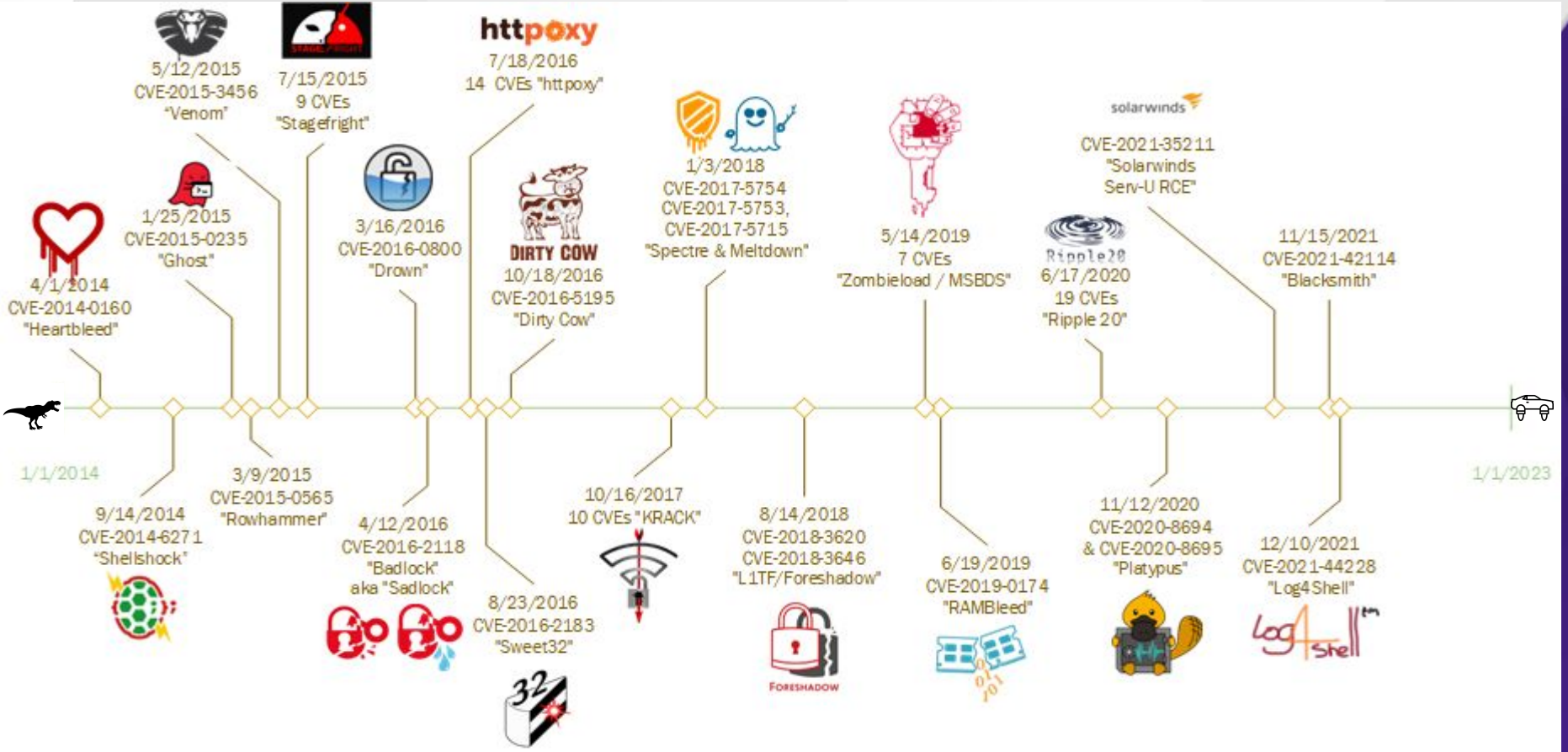
- It is a statement from an organization that hackers engaged in Good Faith Security Research and ethical disclosure are authorized to conduct such activity and **will not be subject to legal action from that organization.**

https://docs.hackerone.com/organizations/safe-harbor-faq.html
https://disclose.io/

Why CVD is important?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

A Tour of Celebrity/Branded Vulnerabilities 2014 - present



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Why CVD?

CVD helps ensure that software maintainers have access to the resources they need to analyse, test, and fix a reported vulnerability.

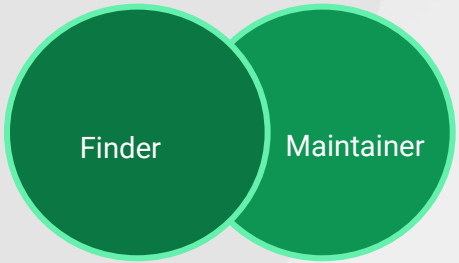
As fixes are developed, authorized trusted parties can assist in testing and staging the patches for **public disclosure** (PD).

At PD, notifications go out to the public and impacted downstream consumers. Everyone has access to the fixes at the same time so that no one group is put at risk more than others. Conversely, no one has pre-access to the bits (so no preference or priority); everyone has equal access.

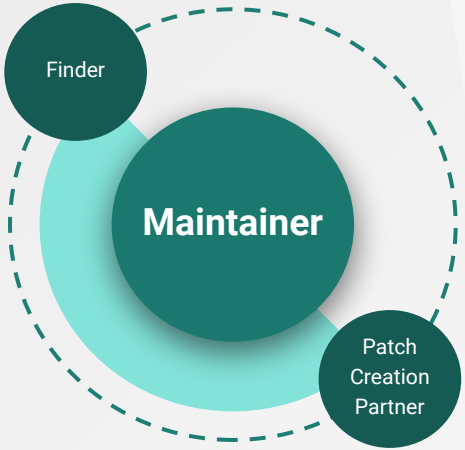
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

CVD can take MANY forms

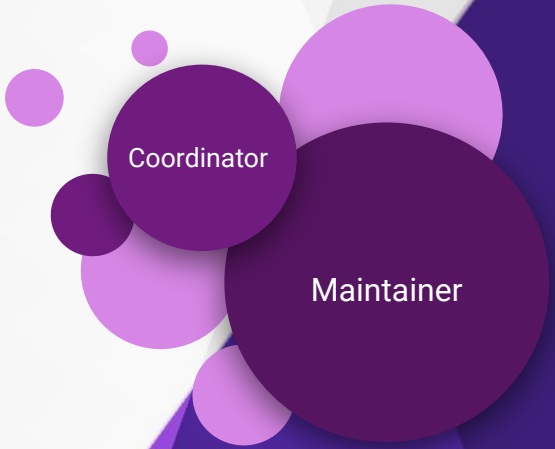
Bi-lateral



Multi-party



Coordinated



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Benefits for OSS of CVD

Adding vital skills/capacity to the remediation process

Broader regression testing/patch review prior to PD

Ecosystem can prepare and stage patches and documentation prior to PD so that **ALL downstream consumers have access to fixes AT THE SAME TIME**

Downstream stakeholders get notification when patches are released

What makes CVD hard?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Why is OSS CVD hard?

Determining how to contact a project is **complicated**

FINDING the appropriate maintainers can be challenging; sometimes upstream **no longer maintains** software

CVD can move **slower** than OSS devs are used to

Response **capabilities or processes** may be lacking

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Why is ~~OSS~~ CVD hard?

Vulnerability disclosure is a human process!

Disclosures can go awry for human-related reasons, like **unavailability** or **inability** to handle or **emotions**

Understanding **motivations** can help drive CVD decisions

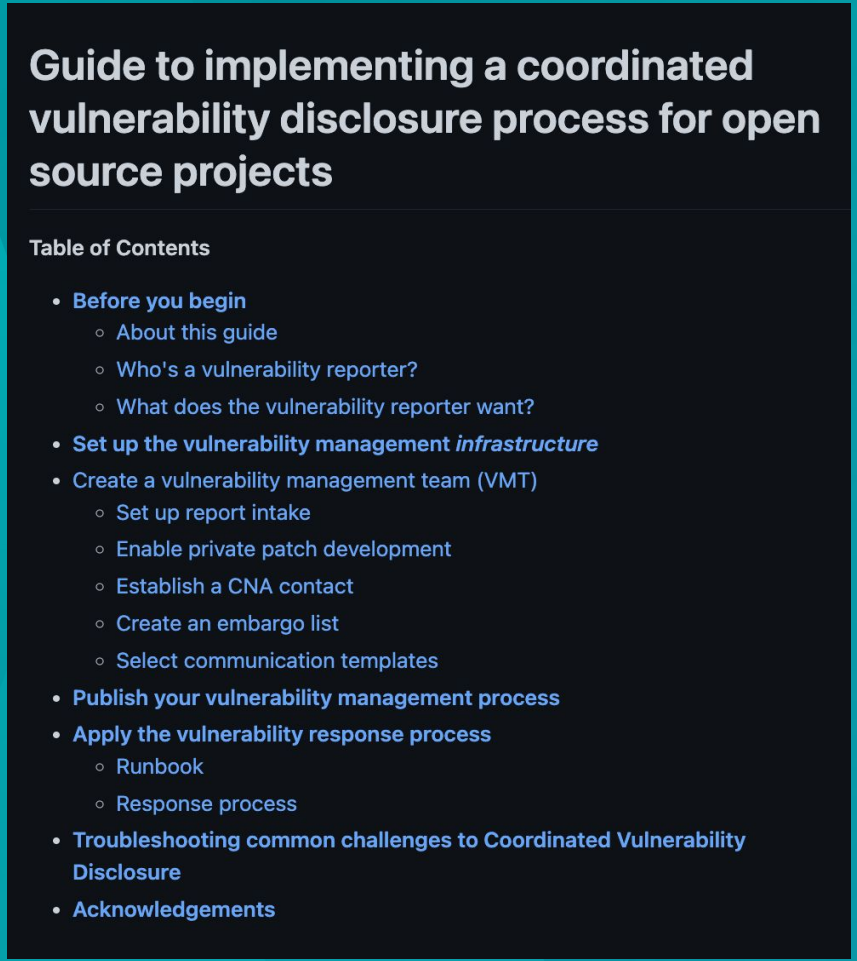
How to do CVD

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The OpenSSF's Vulnerability Disclosure Working Group focuses on these problems.

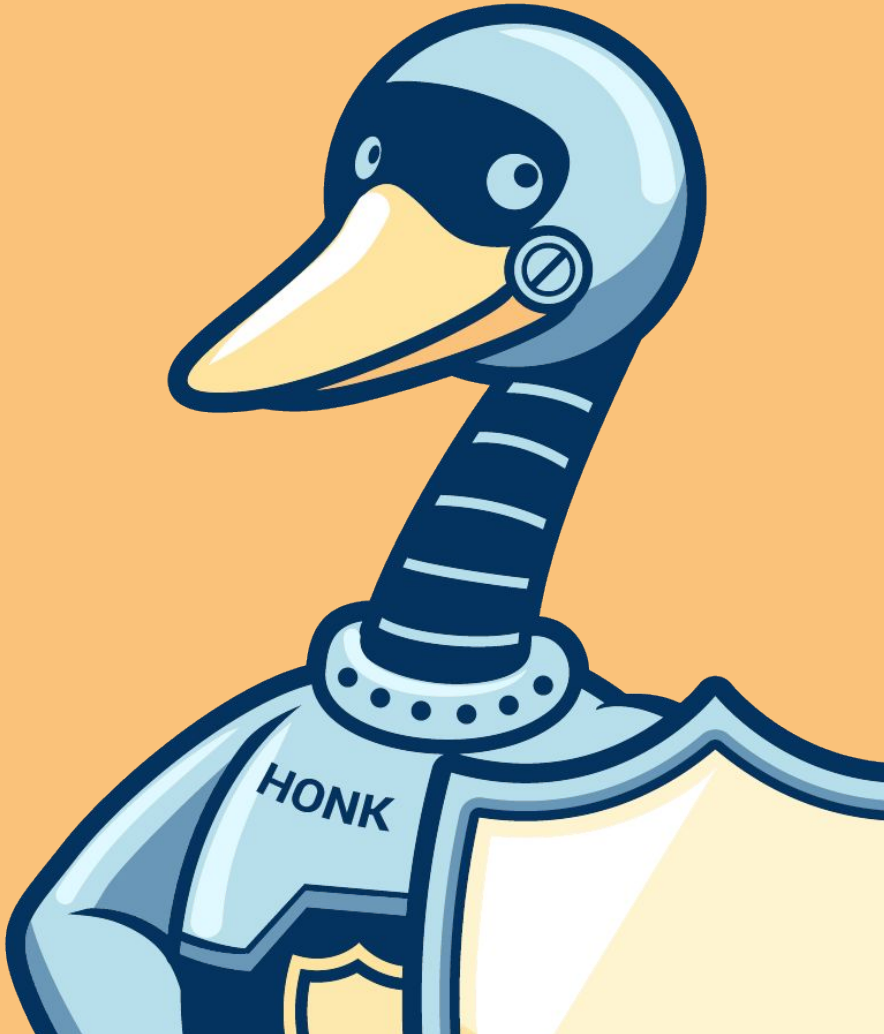
Collectively the group represents developers, suppliers, security researchers, incident responders, coordinators, and vulnerability management practitioners from around the globe.

The group supports and maintains tooling, templates, and best practices guides to help ALL parties involved in CVD within OSS.



https://github.com/ossf/oss-vulnerability-guide/blob/main/maintainer-guide.md
https://github.com/ossf/oss-vulnerability-guide/blob/main/finder-guide.md

Here are some things you to do to set up your project for CVD-success!



Publish your vuln mgmt process/security policy

- Each project operates differently and has different needs.
- Tell people how you want to handle security reports and how they will be managed.

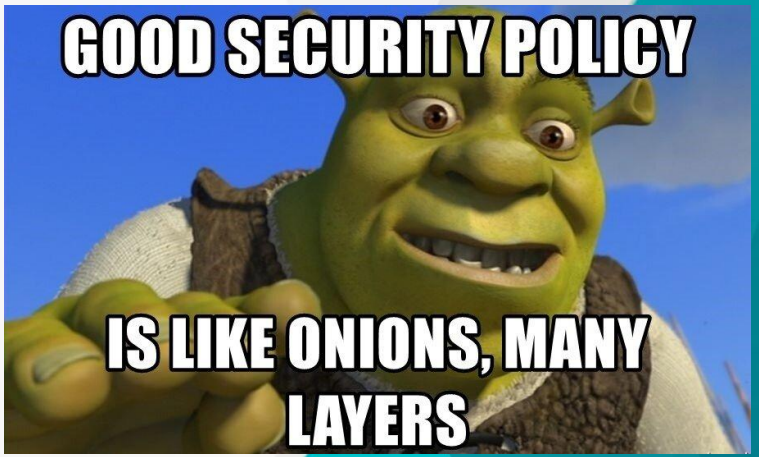


Image Source

https://docs.github.com/en/code-security/getting-started/adding-a-security-policy-to-your-repository
https://gitlab.com/gitlab-org/gitlab-foss/-/blob/read-template-from-repository/doc/release/security.md

Establish your Security “team”

- Not every developer is a securityologist.
- Identify people in your project that might have these skills or find some security friends that can help in times of need!

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Establish a CNA contact (or other means of vuln id disclosure)

- It is important that as vulns are found and fixed that your downstream is told about it so they can take action.
- A CVE Numbering Authority (CNA) is a party authorized to issue CVE IDs for a particular scope of hardware/software, and is the most common way organizations communicate about vulnerabilities.
- There are other ID methods such as GHSA, OSV or GSD that are also CVE-compatible and OSS-workflow-friendly.

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Setup a means for private intake

- A reported vulnerability is a threat to any users of the software if left unfixed.
- Establishing a private way that a Finder can share details or reproducers with the project helps ensure bad actors don't learn about the problem before the project or the users.

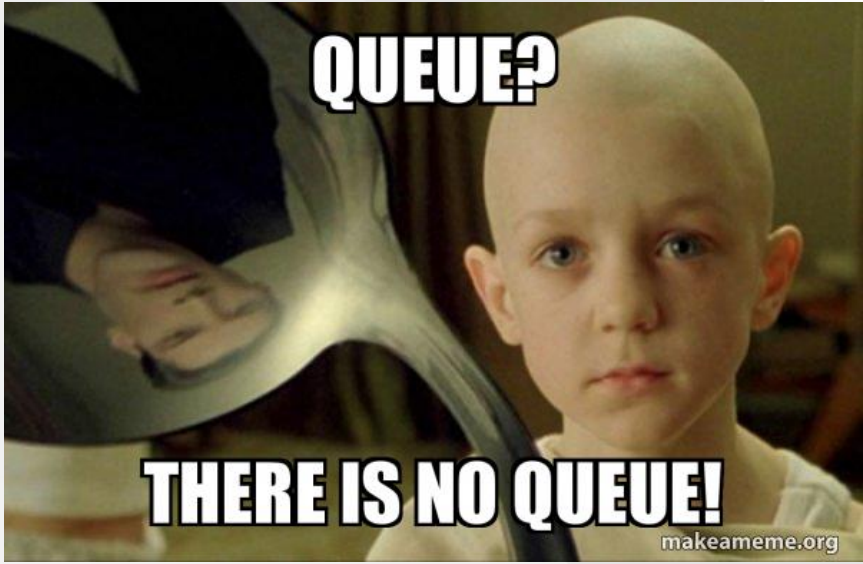


Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Establish a means of private patch development & testing

- Like private reporting, it is important that patches that address the vulnerability be kept out of mainline code branches until **after** they have been tested and are ready for public disclosure.
- Bad actors monitor source code repositories for “interesting” (i.e. security-related) PRs and commits.

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Establish an embargo list

- Depending on the size and scale of the project, you may need to have a pre-authorized list of people/projects that either contribute to your project or are vital to your supply chain.
- Reading these types of people in prior to PD helps ensure that documentation, communications, and patches can be staged so that downstream consumers can get them as soon as the issue goes public.

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Determine how you will communicate the disclosure

- Mailing list, blog, commit comment, VEX statement, full-on security advisory - there are many ways to tell your downstream that there was vulnerability and how to fix it.
- Consider to disclose to places like *oss-security* at PD for broader visibility.

Image Source

What questions do you have?

What additional resources from the WG would you find helpful?

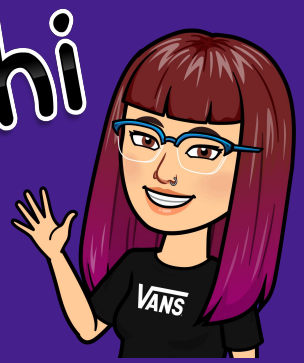
Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Ways to Participate

- Join the OpenSSF Mailing List
- Follow us on Twitter
- Follow us on LinkedIn
- Follow us on Mastodon
- Follow us on Facebook
- Subscribe to our YouTube Channel
- Join a Working Group/Project
- Access the Public Meetings Calendar
- Participate on Slack
- Follow OpenSSF on GitHub
- Become an Organizational Member

Thank You



@taladrane

@taladrane@fosstodon.org

https://github.com/taladrane

https://www.linkedin.com/in/madisonoliver24

CRob_at_Intel_dot_com

@SecurityCRob

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa

https://www.linkedin.com/in/darthcrob/