OpenSSF

OPEN SOURCE SECURITY FOUNDATION

FOSS Backstage
March 17, 2022

Preparing for Zero-Day: Vulnerability Disclosure in Open Source Software

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

[de@FOSS.backstage ~]$ ./HelloWorld.sh

The thoughts and feels expressed here are personally held or experientially earned, and not necessarily those of our employers

Anne Bertucio (@WhyHiAnnabelle)

Representing the Maintainer Persona

- Senior Program Manager in Google's Open Source Programs Office (OSPO)
- Strengthening the security practices of OSS projects run by Google, helping Googlers work in OSS (particularly vuln disclosure!)
- Member of OpenSSF Vuln Disclosure WG
- Previously: Kata Containers and OpenStack contributor, very mediocre bicycle racer

Jennifer Fernick (@enjenneer)

Representing the Finder/Researcher Persona

- SVP & Global Head of Research at security consulting firm NCC Group; has disclosed many, many vulns
- Co-founding Board member of the Open Source Security Foundation
- Previously: Cryptographer (quantum cryptanalysis, post-quantum cryptography, cryptographic standards development, crypto architecture) + security researcher
- Previously: Director of Information Security at a major bank

CRob, n, adj, and v (@SecurityCRob)

Representing the Supplier/PSIRT persona

- Pronunciation: U.S. (K-robe)
- Over 25 years of Enterprise-class Architecture, Engineering, Operations, and Security experience
- Ambassador For Intel Product Assurance and Security
- Working Group lead for the OpenSSF Dev Best Practices & Vuln Disclosure WGs, OSSF TAC, FIRST PSIRT SIG, Bug Bounty COI, and others
- Previously: Program Architect Red Hat Product Security
- Pirate-enthusiast & hat-owner

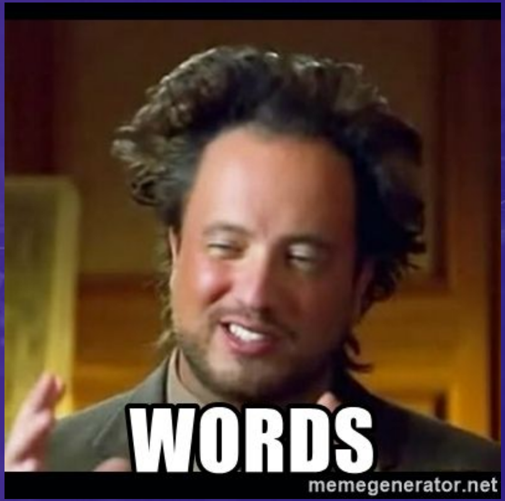
Bug - an error or flaw in computer software that causes incorrect or unexpected results, or unintended behaviour (sometimes referred to as a “defect”)

Vulnerability - is a weakness of software, hardware, or online service that can be exploited and has security implications.

CVE - a unique number given to identify a specific security flaw in a specific piece of software (or firmware, or hardware)

Threat - is the potential cause of an incident that may result in harm to a system or organization

Embargo - the period of time that a security flaw is known privately, prior to a deadline, after which time the details become known to the public



Source - https://memegenerator.net/img/instances/54336027.jpg

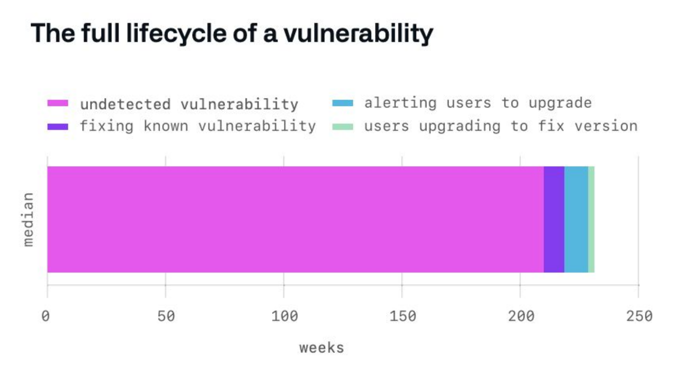
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Not previously known by affected project

Security-related software (or hw) flaw

Q1 - What actually *is* a zero day vulnerability?

Source: GitHub State of the Octoverse 2020 Security Report



- **OSS vulns take years to detect:**
  A typical vulnerability on GitHub goes **undetected for over 4 years** (>2.5 years for critical vulns)
- **OSS vulns take mere days to exploit:**
  Days between vulnerability disclosure and exploit creation has **gone from 45 days down to only 3**

One report found that **84% of FOSS codebases had at least one vulnerability**, with the average having 158 per codebase

2021 Open Source Security and Risk Analysis Report

IMPORTANT!

- All complex software has flaws. If you receive a report of a vuln in your code, don't be ashamed - **what matters most is how you respond & patch!**
- Researchers have options - selling vulns, "dropping" 0day without letting you patch first, or working together to help you patch. **If someone's reaching out to your project, they probably want to help :)**

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

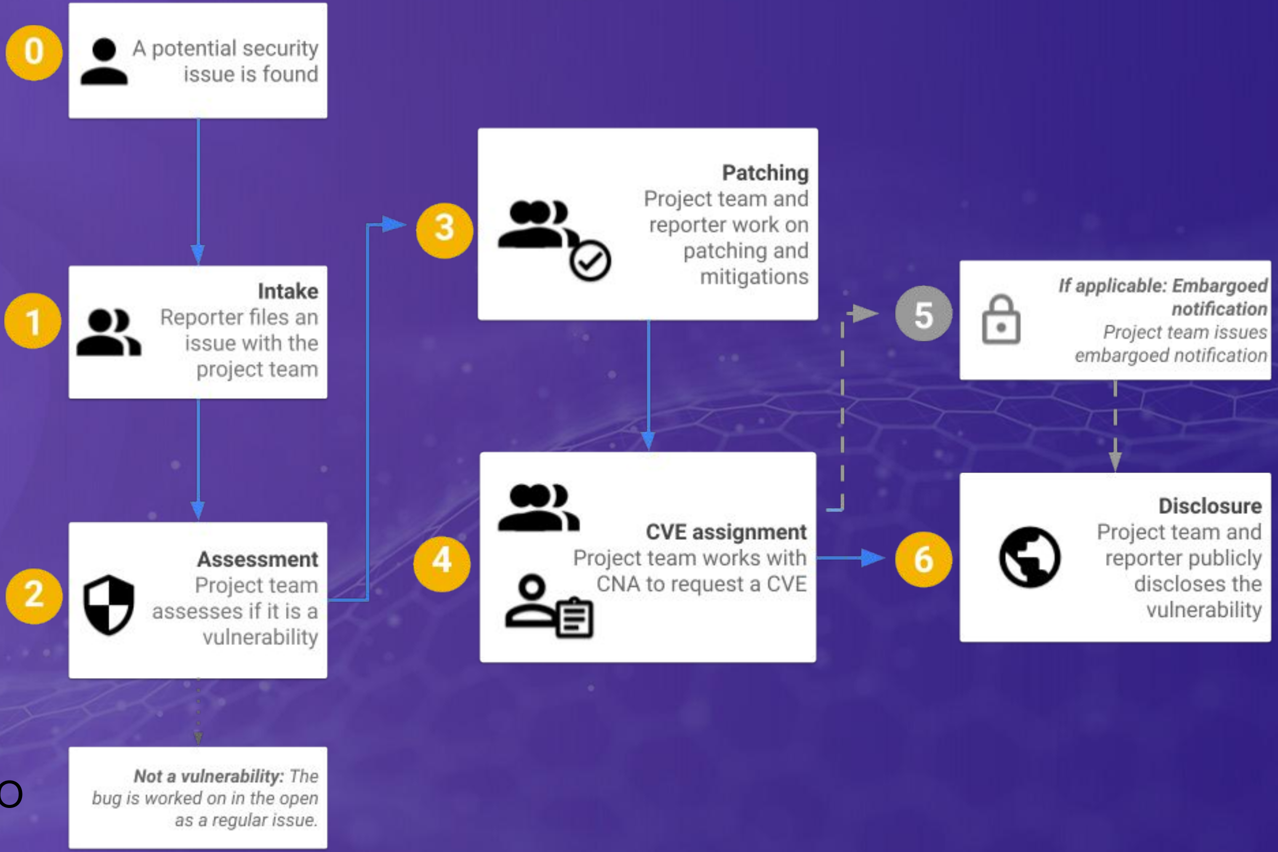
Q2 - How do different projects share vulns (differently)?

Source - https://www.memecreator.org/static/images/memes/5195522.jpg

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Coordinated Vulnerability Disclosure in Open Source Projects



0 A potential security issue is found

1 **Intake** Reporter files an issue with the project team

2 **Assessment** Project team assesses if it is a vulnerability

Not a vulnerability: *The bug is worked on in the open as a regular issue.*

3 **Patching** Project team and reporter work on patching and mitigations

4 **CVE assignment** Project team works with CNA to request a CVE

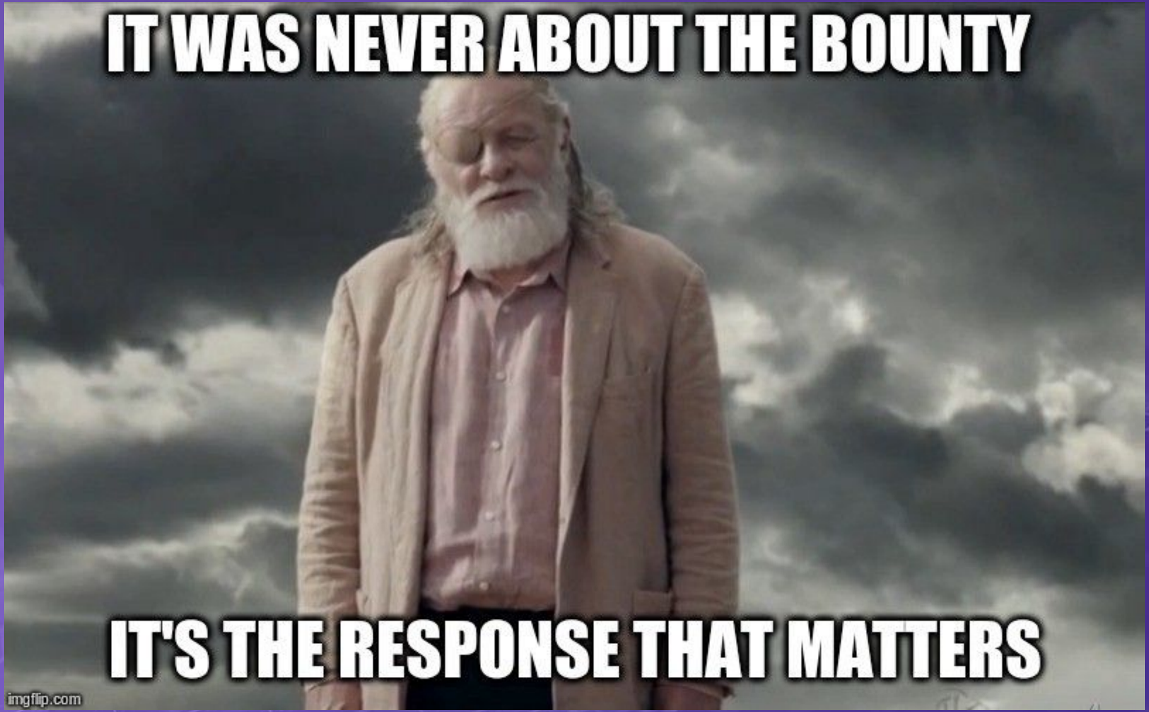
5 ***If applicable: Embargoed notification*** *Project team issues embargoed notification*

6 **Disclosure** Project team and reporter publicly discloses the vulnerability

Source - Google OSPO

✅	❌
● Date of intended patch by project (within typical 30/60/90 day window, ideally) ● Obtaining CVE for bug ● Advisory publication including communications timeline ● Blogging/conference presentation by researcher after bug has been patched	● Researcher asking you for money ● Any kind of extortion / bribery / other sketchy or illegal behaviour ● Privileged access to a developer / project’s systems or infrastructure ● Having the developers/maintainers run code they don’t understand ● Any kind of NDA or other legal agreement ● Researcher dropping 0day *without* basic conditions being met (earnest attempt to contact you; clear communication of vuln, target, and impact; 30/60/90 day disclosure) - however, this can vary by researcher

What to expect from researchers during vulnerability disclosure



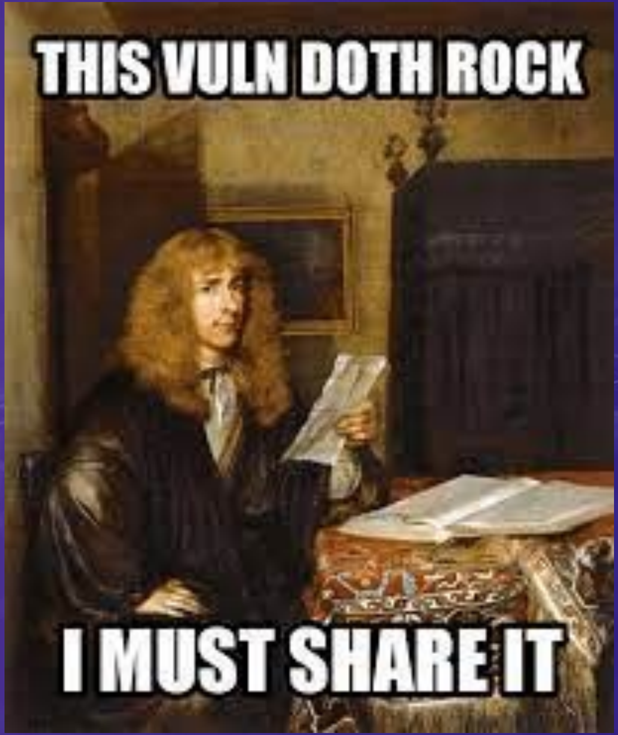
Q3 - What is CVD, VDP, and BB?

Source - https://miro.medium.com/max/1400/1*6x9aWgCHaoszo6OWdS6SNg.jpeg

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Q4 - What are common challenges to coordinated vulnerability disclosure?

- What if I don’t actually think it’s a vuln?
- What if this specific bug can’t be patched, or I don’t know how to write a patch for it?
- What if the researcher and I disagree on publication timelines for vuln release?
- What if a researcher drops 0day on my project?
- What if the vulnerability is believed to be exploited in the wild?



Source -https://www.mogozobo.com/wp-content/uploads/2019/03/127.png

Q5 - What are some lessons learned from CVD over the years? Where could I learn more?

Source https://memegenerator.net/img/instances/82221847.jpg

Recommendations

- Have a security policy (e.g.: security.md file on Github)
- Be contactable (have a security@ email address!)
- Remember, feedback is a gift
- Communicate every step of the way, and ask questions about things you don't understand
- There are a lot of great tools to help (ZAP, Dependabot, etc.)

Source - https://media.makeameme.org/created/1010-would-recommend-d1dc8aa5ab.jpg

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Source https://memegenerator.net/img/instances/73318650.jpg

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Get Involved

- Join a Technical Working Group - https://github.com/ossf
- Join the Mailing List - subscribe to the openssf-announcements mailing list
- Join our Public Meetings - https://bit.ly/ossf-calendar
  Next OpenSSF Vuln Disclosure Group meeting March 21st. 4-5pm US Eastern, all are welcome!
- Join our Slack Channel - https://slack.openssf.org
- Watch YouTube Channel - https://bit.ly/ossf-youtube
- Feedback?
  - Drop us an email! - operations@openssf.org

Useful Resources about Vulnerability Disclosure

OpenSSF Coordinated Vulnerability Disclosure Guide:
https://github.com/ossf/oss-vulnerability-guide/blob/main/guide.md

Basics about CVEs
https://www.cve.org/About/Overview

National Vulnerability Database (NVD) of existing vulnerabilities
https://nvd.nist.gov/

Examples of Technical Advisories published by security researchers
https://research.nccgroup.com/category/technical-advisory/

Example Disclosure Policy from a research group (two examples with different terms)
https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html
https://research.nccgroup.com/wp-content/uploads/2021/03/Disclosure-Policy.pdf

Thank you!

openssf.org/getinvolved
github.com/ossf

	@whyhiannabelle	@enjenneer	@SecurityCRob
	annabellegoth2boss	jenniferfernick	SecurityCRob
		NCC Group Research Blog	The Security Unhappy Hour

OpenSSF
OPEN SOURCE SECURITY FOUNDATION