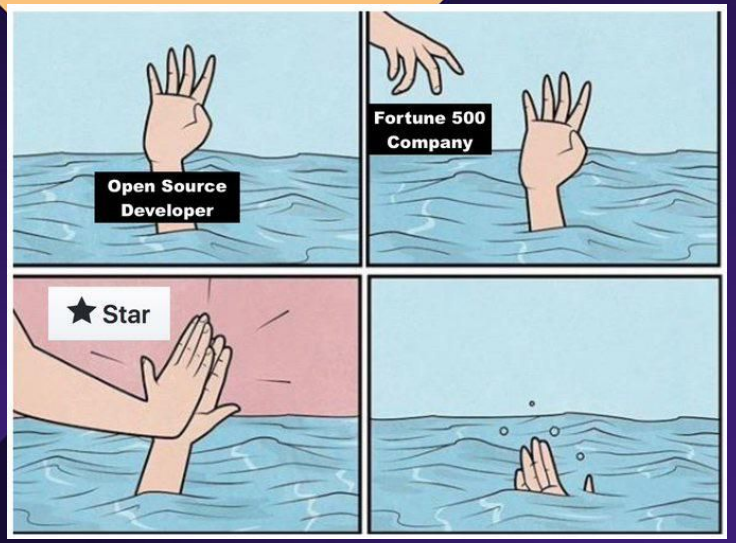
Drowning and Angry



Open Source Project Vulnerability Handling in the Era of AI Slop reports

CRob - OpenSSF Chief Security Architect

Vuln4Cast - Sept 26, 2025

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

ABSTRACT

The vulnerability management ecosystem has long had challenges effectively engaging with Open Source Software projects and maintainers. The advent of easy access to low/no-cost AI tools has exponentially increased the volume of defect reports to vendors and to upstream. Sadly, unlike a commercial enterprise or vendor, upstream open source maintainers are not equipped to deal with this new deluge of "helpful" reports, the overwhelming majority of which are low-quality reports that actually slow the developers down from addressing actual vulnerabilities that could have real-world impacts.

The session will dive into the deep end of things and showcase several recent interactions between upstream developers and the army of AI "researchers" and highlight how this new trend threatens to further erode the interest and ability of upstream maintainers from participating in vulnerability response. We will discuss potential solutions and best practices for managing this influx of data, ensuring that valuable contributions are not lost in the noise, and fostering a more sustainable engagement model between security researchers and open source communities. This includes exploring strategies for filtering, prioritizing, and automating the initial assessment of AI-generated reports, as well as promoting clearer communication guidelines for responsible disclosure.

Who is this guy?

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

```
# chmod 666 crob.md
```

44th level Dungeon Master

27th level Securityologist

Pirate-enthusiast & hat-owner

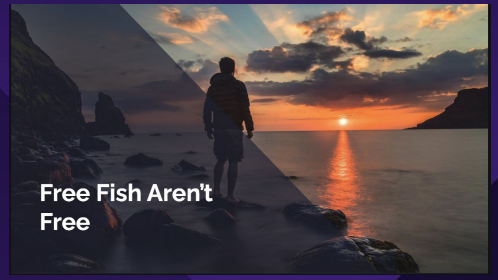
Chief Technology Officer & Chief Security Architect, OpenSSF - Linux Foundation

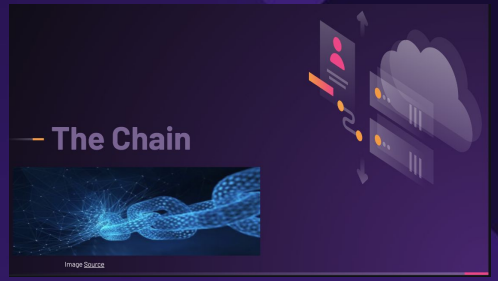
Involved in upstream OSS CVD for ~15 years

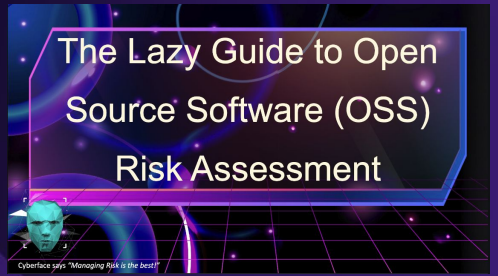
Most images generated by Microsoft Designer and ChatGPT, except that -> That's just my pal Gimp!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Prior Art







https://github.com/SecurityCRob/presentations/tree/main

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The Dream of CVD....

Finders notifying Maintainers and responsible Manufacturers who all collectively work together to release fixes and guidance at a mutually agreed-upon Public Disclosure (PD) date.

All stakeholders have timely access to fixes and documentation to evaluate their own exposure and collectively the ecosystem has a common reference for that particular problem.

The reality of CVD

Antiquated systems steeped in bureaucracy.

Lack of public information to adequately contact responsible parties.

Difference in “Product” vs. “Project” capabilities and processes.

Overall lack of transparency in the process.

Gulf in understanding how the stakeholders operate across the ecosystem.

CVE CNA “Fun Facts”

As of Sept 18, 2025, there were **470** entities listed as CVE Numbering Authorities (CNAs) in the CVE program

Of those, **205** mention “open source” somewhere in their profile

Of those, **56** generously could be considered very OSS-adjacent/involved

Broadly, with a few exceptions, those entities state something like this about their scope:

“<vendor> products and vulnerabilities in third-party software discovered by <vendor> that are not in another CNA’s scope .”

WUT is OSS?

There isn't a single, exact figure for the total number of open source projects in 2025, but data suggests the number is in the hundreds of millions, with over 518 million on GitHub alone as of 2024

518 million+ > 205

That’s a HUGE gap between those creating software and those consuming and reporting about it!

Some OSS “Fun Facts”

There is NO such thing as THE Open source

OSS & CVE

Not every maintainer of project needs to nor wants to be a CNA. Open Source Foundations (aka CRA Stewards) often perform these services for projects in their community.

- Apache Software Foundation: 350+ projects
- The Eclipse Foundation: 425+ projects.
- The Linux Foundation: 1,000+ projects

518 million+ > ~2000

Trends in the ecosystem & OSS

The first half of 2025 saw a **16% increase** in CVEs compared to the same period in 2024, rising to 23,667 in total.

86% of commercial codebases **contain vulnerable open source components**, and **81%** of these vulnerabilities **were classified as high or critical** in severity.

The average application contains **over 900 open source dependencies**, many of which are outdated and pose a security risk.

CISO "Fun Facts" Sheet

Growing Threats & Vulnerabilities

Increased Supply Chain Attacks: Expect more sophisticated and frequent attacks targeting the OSS supply chain, as evidenced by incidents like the XZ Utils backdoor, leading to a greater sense of urgency to implement continuous monitoring and advanced tools.

Malicious Packages: The volume of detected malicious open source packages, including those for data theft, has skyrocketed. Attackers increasingly use tactics like dependency confusion, typosquatting, and repository takeovers.

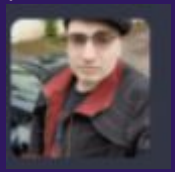
Vulnerable Components: A high percentage of codebases contain vulnerable and outdated open source components, highlighting the persistence of unpatched issues and the need for timely updates and diligent maintenance.

But.....

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

“I’m not a supplier”

Thomas Depierre
Expert Open Source Developer



I am not a supplier

31 Dec 2022 - Thomas Depierre

For the past few years, we have seen a lot of discussions around the concept of the Software Supply Chain. These discussions started around the time of LeftPad and escalated with multiple incidents in the past few years. The problem of all the work in this domain is that it forgets a fundamental point.

Before we get there, I am going to define what is usually meant by Supply Chain and suppliers, why we are applying to software. And then why attempts at bringing FOSS under that definition are deeply misguided.

https://www.softwaremaxims.com/blog/not-a-supplier

TL/DR: Open Source Software is provided “As Is” with no warranty or support; OSS devs have no relationship with or obligation to downstream consumers

Dan Appelquist
Open Source Standards Expert

DEVSECOPS | OPEN SOURCE

When software isn’t a “supply”

Daniel Appelquist
February 15, 2023

Editor’s note: The following think piece, written by Snyk’s Open Source and Open Standards Strategy Director, Daniel Appelquist, examines the origin of the term “supply chain security” and whether it’s a good fit for today’s open source software development process.

https://snyk.io/blog/when-software-isnt-a-supply/

TL/DR: Our words have meanings; the industry should redefine our terminology

Dr. David A. Wheeler
Prolific Open Source Security Expert

Distinguish between supplier and vendor

David A. Wheeler, The Linux Foundation, < dwheeler at linuxfoundation dot org >

I think it’s important to distinguish the term “**supplier**” (any source of a good or service) from the term “**vendor**” (a supplier who is paid and has a contractual relationship). Here’s why.

https://openssf.org/blog/

TL/DR: Words matter; OSS Devs ARE the “source”, but not necessarily “vendors” with contracts & obligations; there are means for consumers to get support of OSS

Brief Tour of Supply Chain Attacks through the years....

<- The “OG” Supply Chain attack 1194–1184 BC

<- Typically the 1st time “supply chain attack” was recognized as an issue in cybersec

https://www.sonatype.com/resources/vulnerability-timeline
https://www.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks
https://linuxfoundation.eu/newsroom/the-rising-threat-of-software-supply-chain-attacks-managing-dependencies-of-open-source-projects

Supply Chain attacks, evolved

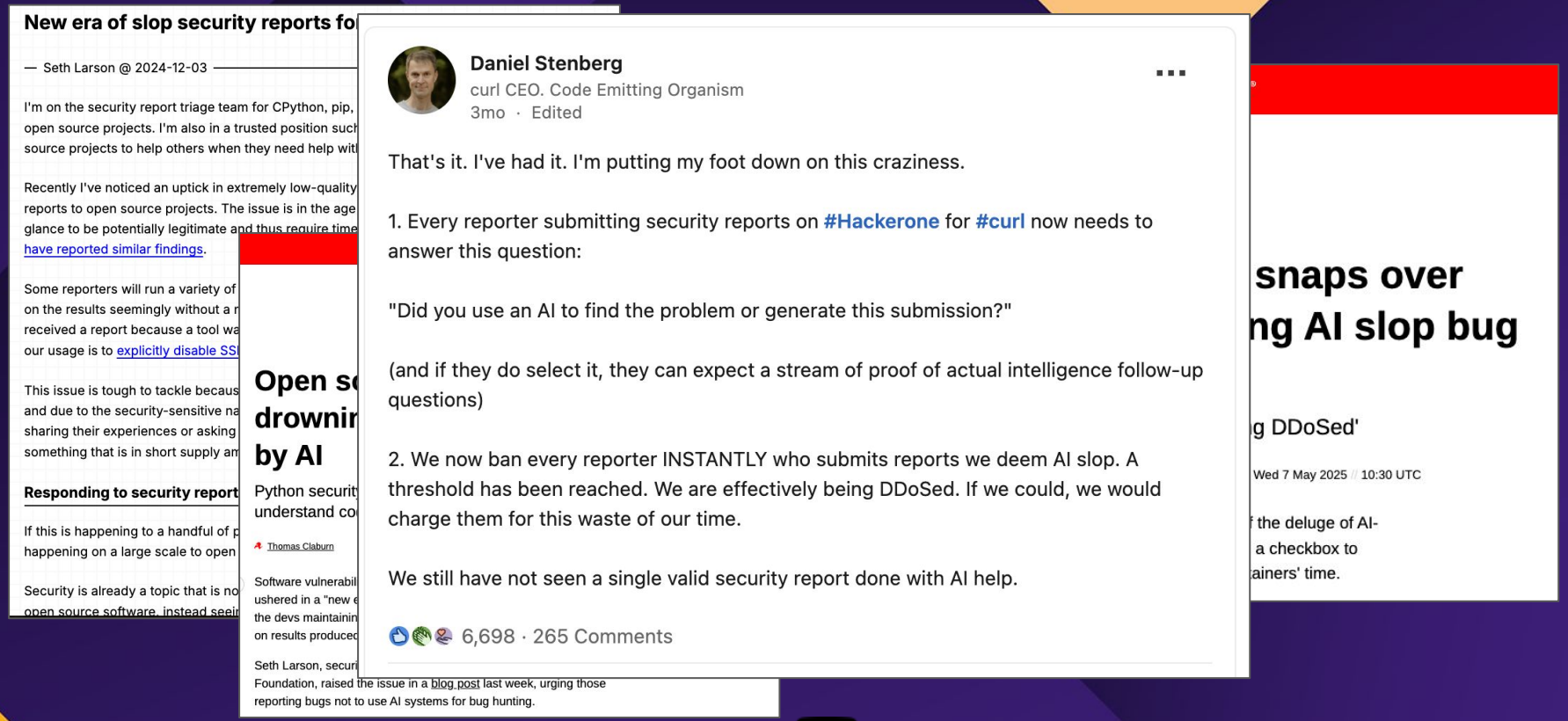
https://www.sonatype.com/blog/ongoing-npm-software-supply-chain-attack-exposes-new-risks
https://www.darkreading.com/application-security/self-replicating-shai-hulud-worm-npm-packages

“AI enters the Chatroom”

The Rise of AI and extreme pressure it puts on the already fragile system

- AI Tooling allows **more** researchers the ability to look at **more** things in much shorter periods of time.
- High Volume of “findings.”
- Prone to Hallucinations (including bogus dependencies citations “slopsquatting”).
- Trained on publicly available code of varying degrees of quality.
- Overall upstream consensus is these reports add little to no value.

But don’t just take CRob’s word on it.....



New era of slop security reports fo

— Seth Larson @ 2024-12-03 —

I'm on the security report triage team for CPython, pip, open source projects. I'm also in a trusted position such source projects to help others when they need help with

Recently I've noticed an uptick in extremely low-quality reports to open source projects. The issue is in the age glance to be potentially legitimate and thus require time have reported similar findings.

Some reporters will run a variety of on the results seemingly without a r received a report because a tool wa our usage is to explicitly disable SS

This issue is tough to tackle becaus and due to the security-sensitive na sharing their experiences or asking something that is in short supply am

Responding to security report

If this is happening to a handful of p happening on a large scale to open

Security is already a topic that is no open source software, instead seein

Open s
drownin
by AI

Python securit
understand co

Thomas Claburn

Software vulnerabil
ushered in a "new e
the devs maintainin
on results produced

Seth Larson, securi
Foundation, raised the issue in a blog post last week, urging those reporting bugs not to use AI systems for bug hunting.

Daniel Stenberg
curl CEO. Code Emitting Organism
3mo · Edited

That's it. I've had it. I'm putting my foot down on this craziness.

1. Every reporter submitting security reports on #Hackerone for #curl now needs to answer this question:

"Did you use an AI to find the problem or generate this submission?"

(and if they do select it, they can expect a stream of proof of actual intelligence follow-up questions)

2. We now ban every reporter INSTANTLY who submits reports we deem AI slop. A threshold has been reached. We are effectively being DDoSed. If we could, we would charge them for this waste of our time.

We still have not seen a single valid security report done with AI help.

6,698 · 265 Comments

snaps over
ng AI slop bug

g DDoSed'

Wed 7 May 2025 // 10:30 UTC

f the deluge of AI-
a checkbox to
ainers' time.

[AI slop attacks on the curl project - Daniel Stenberg]

What DEVs HATE about AI slop

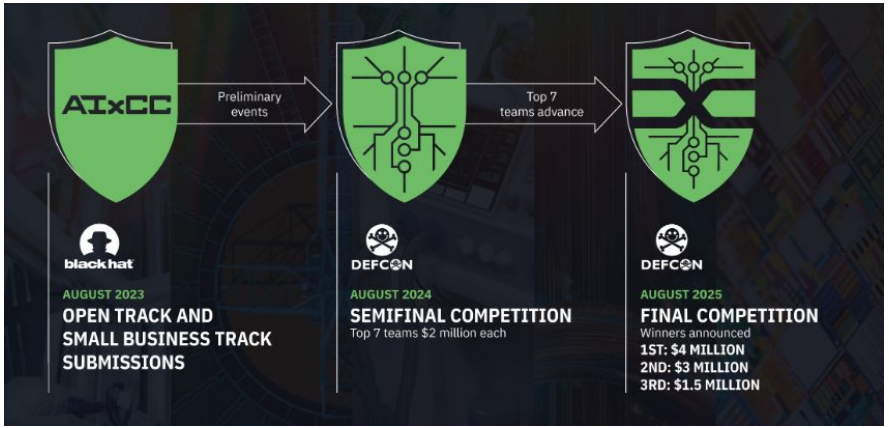
- AI is good at simple coding tasks, but AI does not understand complex codebases.
- Unscientific review of current AI Slop shows that <5% of reports are valid issues.
- AI reports are incredibly verbose.
- AI vuln reports (through Bug Bounties or normal means) are “DDoS”’ing projects (**each report takes 1-4 hours on average to triage**, and when they don’t represent ACTUAL bugs, this hinders the project’s ability to deliver features and actual fixes).
- Hallucinations, slopsquatting

We are at an AI crossroads

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

AIxCC - Saviour of the Ecosystem or Harbinger of DOOM?!?

- Two-year competition that rewards autonomous systems that find and patch vulnerabilities in source code.
- The challenges are well-known open-source projects.
- The vulnerabilities are realistic or real.
- Patching is worth more than finding.
- Code & data released as open source.



AIxCC FINALS RESULTS

Automated patch development is:
Fast, Scalable, Cost-effective, Available/Open-source

REPOSITORIES
28

CHALLENGES
53

KNOWN VULNERABILITIES DISCOVERED
77% (54/70)

KNOWN VULNERABILITIES PATCHED
61% (43/70)

AVERAGE TIME TO PATCH
45 minutes

TOTAL LINES OF CODE ANALYZED
54M

COST PER TASK SUCCESS
~$152

TOTAL SPENT (COMPUTE + LLM)
$359K $277K Compute, $82K LLM

TOTAL LLM QUERIES
1.9M

REAL WORLD VULNS DISCOVERED
18

FOUND IN C
6 0 patched

FOUND IN JAVA
12 11 patched (3 without PoV)

TEAM	TEAM TOTAL SCORE	% CORRECT SUBMISSION (ACCURACY)
Team Atlanta	392.76	91.27%
Trail of Bits	219.35	89.33%
Theori	210.68	44.44%
All You Need IS A Fuzzing Brain	153.70	53.77%
Shellphish	135.89	94.83%
42-b3yond-6ug	105.03	89.23%
Lacrosse	9.59	42.86%

AIxCC & Cyber Reasoning Systems Learnings

- Scope the AI tools to specific purpose. Don't present a whole codebase to an LLM and say "go"
- Leveraging multiple techniques yields better results
- Fixes are more valuable than finding
- Provide a proof of vulnerability
- Human review & verification, no blind trust
- View AI-suggested dependencies with **EXTREME** suspicion
- Meet projects where they are / follow the project's practices for reporting

OpenSSF Critical Projects Maintainer Support Program

Gather: Collect information on the bugs that were found and available patches

Curate: Evaluate bugs and patches, review & prioritize, validate

Outreach: Initiate communication with the project

Iterate: Work through process with project toward successful patch acceptance

Support: Review more findings, provide options for deeper support:

- oss-fuzz harnessing
- Make AIxCC tools available to project
- Security audit
- Remediation work
- Backlog help

AND we all have THIS to look forward to....

Downstream already demands much of their upstream creators.

Imagine what this will look like as legal obligations like the EU CRA comes online combined with AI-"Researchers" "helping".

Ways to get involved

- VulnWG + AI/ML WG AI slop concise guide
  - https://github.com/ossf/wg-vulnerability-disclosures
- OpenSSF Cyber Reasoning Systems SIG (established Sept. 2025!)
  - Cyber Reasoning SIG Slack
- Finder Guidance on working with Upstream
  - https://github.com/ossf/oss-vulnerability-guide/blob/main/finder-guide.md
- Code of Conduct for AI tool usage
  - https://github.com/ossf/ai-ml-security

Thank You

CRob_at_OpenSSF_dot_org

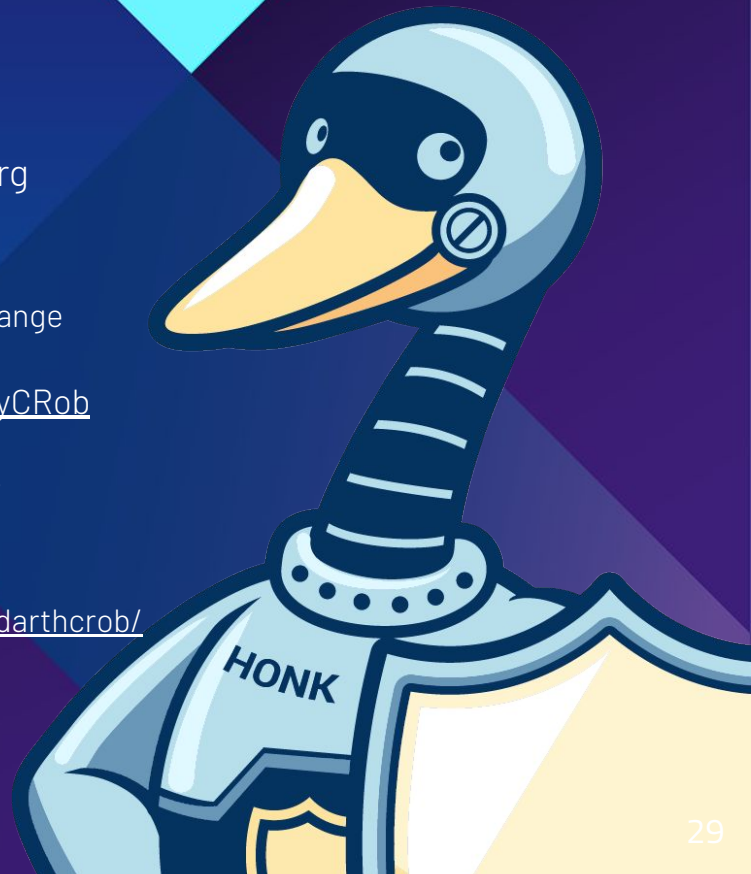
@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

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



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Legal Notice