UnlockOpen

The Missing Postmortem

OWASP BeNeLux days

December 2025 – Mechelen, Belgium

Tobie Langel, Principal
tobie@unlockopen.com

In April 2024, the OpenJS Foundation, home to open source projects used by billions of website, announced it had intercepted a potential open source project takeover attempt similar to XZ Utils.

Tobie Langel, Principal
tobie@unlockopen.com

This is its missing post-mortem.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Have you dealt with a vulnerability

1. in your code base?
2. in your open source project?
3. in someone else's open source project?

Tobie Langel, Principal
tobie@unlockopen.com

Have you dealt with a security incident

1. in your organization?
2. in someone else's organization?
3. in an open source project?
4. involving multiple, unrelated open source projects?
5. involving multiple, unrelated high-profile open source projects?

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Well, I did.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Who am I?

Tobie Langel

🎶 Jazz drummer → open source dev → consulting

💼 UnlockOpen, open source strategy consulting firm

🪑 CPC Vice Chair & Board Director OpenJS

❌ No security background

🛡️ Open Regulatory Compliance (ORC) WG

🇪🇺 EU CRA Expert Group

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

🎯

Targeted Project

- 🌐 Widely used JavaScript project *(critical infra)*
- 🔬 High-impact, low-visibility dependency
- 😰 Single exhausted maintainer

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Timeline

- 🔎 Predating suspicious activity (before Q3 2023)
- 🗜️ Pressure campaign starts (Q3 2023)
- 📝 XZ Utils backdoor announced (March 29, 2024)
- 🛡️ Project secured
- 🌐 Broader ecosystem risk identified
- 🏛️ Escalation to CISA
- ⏳ The Stall
- 💡 The Lightbulb moment
- 😰 The Scramble

Tobie Langel, Principal
tobie@unlockopen.com

Predating suspicious activity

Months before anything started:

- 🚩 Odd and/or low-quality pull requests: e.g. replacing boolean `false` with string `"false"` in tests (equivalent to `true` in JS)
- 😈 Possible motivations:
  - **Positioning** - establish a contribution history
  - **Test evasion** - weaken guardrails for future changes
- 👀 Individually harmless, but collectively?

Tobie Langel, Principal
tobie@unlockopen.com

Pressure campaign

- ⚠️ Strong resemblance to early XZ Utils patterns
- 📨 Multiple emails send to community representatives, Cross Project Council (CPC) mailing list, and project maintainers over months
- 🎭 Multiple identities, overlapping language, sometimes nearly verbatim copies of emails
- 🔁 Repeated themes: *“Project is unmaintained”*, *“Security vulnerabilities must be fixed”*, *“The foundation should appoint new maintainers”*, etc.
- 📝 Noteworthy: Pull request appeared **within 24 hours** of us replying to an email after *months* of silence.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

XZ Utils backdoor announced

- 🤔 Had found those emails suspicious previously
- 💡 But that's when it clicked!
- 👉 Later, we found out the emails to the CPC mailing list where bouncing and I was one of the only one getting them besides the maintainers

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Project secured

- Securing the project was fairly quick
- Maintainer had been maintaining a tight ship
- Knew maintainer from way back, trust already established
- Lucky to have security expert on staff paid by the Sovereign Tech Fund for a different project
- escalated to OpenSSF & Linux Foundation

Tobie Langel, Principal
tobie@unlockopen.com

Broader ecosystem risk identified

- ⚠️ Identified contribution from threat actors in other OpenJS projects
- 🚨 Threat actors listed as maintainer in multiple, high-profile JS projects outside of OpenJS
- 💀 Threat actors listed as maintainer in high-profile C projects used by about a billion of consumers

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Escalation to CISA

- Concerned this wasn't taken seriously enough
- Reached out to personal contact at CISA
- Joined CISA's Joint Cyber Defense Collaborative Partner Program (with my company!)
- Invited to shared Slack channel used to coordinate XZ Utils incident

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

The Stall

- ❓ And then… nothing happened!
- 👨‍💻 A few folks I knew from the industry that were in the channel helped investigate a bit, but that was it.
- ❌ No support from anyone besides providing a shared channel.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

The Lightbulb moment

- This is were the security expert we had on staff played a critical role by explaining what was going on.
- CISA's role is vulnerability and incident coordination, not intelligence gathering.
- Intelligence gathering is the role of… the intelligence community (FBI in the US).
- Except there was not enough there to launch an investigation.
- Usually, Security Operations Center (SOC) investigate internally.
- Collected evidence allows for intelligence community involvement.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

We were on our own.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

The Scramble

- OpenSSF & LF wanted to make a public announcement to warn maintainers
- All targeted projects needed to be informed urgently. No one was there to do it.
- Leveraged personal network to reach out.
- Had to figure out who was trustworthy, and who wasn't, by myself.
- CISA then just trusted those folks without further vetting.

Tobie Langel, Principal
tobie@unlockopen.com

What's a post mortem for?

Tobie Langel, Principal
tobie@unlockopen.com

“Identify the causes of a project failure (or significant business-impairing downtime), and how to prevent them in the future.” (Wikipedia)

Tobie Langel, Principal
tobie@unlockopen.com

So let’s give it a try!

Tobie Langel, Principal
tobie@unlockopen.com

The Gap

We know how to handle **vulnerabilities.**
We do *not* know how to handle **incidents** in open source.

- CVEs, coordinated disclosure, patches → mature
- Social engineering, impersonation, multi-persona attacks → no playbooks
- FOSS has long assumed it wasn't a target
- Attackers no longer share that assumption

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

No open source SOC

🏛️ Governments assume every organizations has a SOC

❌ There's no SOC for open source

👉 Open source incidents fall in a conceptual gap between SOCs and CSIRTs.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Other wrong assumptions about open source

- ❌ Vetted employees
- ❌ Control and surveillance of the computers and network used by developers
- ❌ All developers work for the same organization
- ❌ All developers work for a single organization

Tobie Langel, Principal
tobie@unlockopen.com

Trusted introduction model fails for open source

- CSIRTs rely on **trusted introductions**
- Intros assume institutional vetting
- In open source, intros are personal and informal
- In our case, intros were **over-trusted**
- CSIRT processes assume corporate vetting structure. Open source doesn't have that

Tobie Langel, Principal
tobie@unlockopen.com

Additional gaps

- No place to send “something feels wrong”
- No cross-ecosystem warning channels
- Personal relationships fill the role of institutional processes
- No entity able to request or trigger a forensic investigation

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Why this matters now

- Cyber Resilience Act (CRA) formalizes notification requirements for both vulnerability and incidents
- Supply Chain Attacks are an increasing threat
- Attackers specifically target open source maintainers leveraging burnout, trust and process gaps
- We need to address theses issues

Tobie Langel, Principal
tobie@unlockopen.com

Closing

We have mature processes for vulnerability handling. We have **nothing** for incidents management in open source.

Our whole incident response model is based on primitives that don't exist in open source. We need to identify them and address them.

Until we fix the structural void, the next XZ Utils-style attack may not be caught in time.

Tobie Langel, Principal
tobie@unlockopen.com

UnlockOpen

Tobie Langel, Principal
tobie@unlockopen.com

