EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 5 · 4 September 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Priya Raman (guest) · Jessy Lang

It's Not My Code

Seven rules for depending on code you did not write and do not pay for

A four-day incident ended at a library of forty lines, written nine years ago by one unpaid maintainer who never knew she was load-bearing. Every company that used it extended trust without becoming her customer. The fix is not "pay Priya more", it is "stop being surprised she exists", and that starts with knowing what you depend on.

UNPAID TRUST
Trust without a relationship or a budget.

1. Are we affected, and where?

2. Is the flaw reachable?

3. Do we know the maintainer's name?

RULES FOR WHAT YOU SHIP AND WHAT YOU DEPEND ON

1	**No bill of materials** Four days of investigation instead of four minutes.	Keep an SBOM of exactly what you shipped, version by version, transitively, so that "are we affected, and where" is a lookup. Require vendors to disclose sub-dependencies. The tooling is mostly automatable, mostly your job, and increasingly a CRA expectation.
2	**A fix nobody recognises** The one sentence you need sits in a changelog.	Identify the vulnerable function and let a tool tell you which products contain it, instead of diffing tags by hand. Maintainers: for a real flaw, request the CVE yourself, or someone downstream will do it badly, months later.
3	**Fake critical reports** Full severity score, no proof, no reachability check.	Before you type "critical", confirm the code path is reachable and include a proof of concept. Check a scanner finding against the current package before you open a ticket. Every report costs a maintainer an unpaid evening.
4	**"Unvetted", said afterwards** Blame lands on someone who never signed up to be vetted.	Decide to depend on a component on the record: the SBOM says which library, which version, and why. Own that decision going in, not after. The licence says no warranty, use at your own risk.
5	**Free labour, four payers** Low thousands of companies used it, four ever paid.	Make support a line item somebody is accountable for, because goodness does not survive a budget cycle. Let the security team, not only procurement, read the SBOM, find the load-bearing libraries on a quiet day and approach the maintainer with a support contract, not a bug report.
6	**Paying is not seeing** Funding fixes the unfairness, not the blindness.	Do both: fund the maintainer and keep your own inventory. A generous sponsor still panicked over a different library. One person cannot promise a four-hour response at two in the morning, so "pay Priya more" is not an SLA.
7	**Blind in both directions** Maintainers do not know who depends on them either.	Maintainers: keep an SBOM of your own library's dependencies, so the answer fits in one file instead of an afternoon, and know what depends on you. A visible hospital intake system tells a finder that this is worth escalating.

THREE TAKEAWAYS

Ask the name question
Does anyone here know the name behind your key dependencies? If not, that is where Tess goes first.

Build the list before the incident
It decides whether the next one costs your PSIRT four minutes or four days.

Be found on a quiet Tuesday
Look for the libraries you rely on when nothing is burning, not on the fourth day of an incident.

Listen to the episode
It's Not My Code and the rest of the series.
eacg.de
/en/podcast/s05-not-my-code

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH