OPEN SOURCE SecurityCon EUROPE

Upstream Collaboration for the Win (of the CRA)!

Jan Melen, Ericsson Software Technology
Georg Kunz, Ericsson

Who Are We?

Georg Kunz
Open Source Program Office @ Ericsson

Jan Melén
General Manager @ Ericsson Software Technology

The Cyber Resilience Act

Selected obligations of manufacturers…

Obligations for Manufacturers

- Article 13 (5) – Exercise due diligence

> *For the purpose of complying with paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements, including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.*

Obligations for Manufacturers

- Article 13 (6) – Sharing vulnerability fixes

> *Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex 1. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.*

Obligations for Manufacturers

- Article 13 (8) – Effective vulnerability handling

Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I

Corporate Incentives Shift

- Zero CVE goal may reduce business incentive to utilise Open Source
- Avoid GPL and copyleft license management burden *

- AI-coding buddies simplifies the process of creating the bare minimum (open) source
- AI reduces the marginal cost of re-implementation, weakening the economic advantage of upstream collaboration.

- Less dependencies → lower risk → reduced appetite for shared commons

* Linux Kernel will soon be MIT-licensed and Copyleft will be dead in 5 years

Future Scenarios

OPEN SOURCE SecurityCon EUROPE

Balkanisation and Collapse

OPEN SOURCE SecurityCon EUROPE

- Legal and geopolitical risk overwhelms shared governance
- Major projects hard-fork permanently
- Corporate contributors go private
- Corporates use 3PP vendors to satisfy their dependences
- Volunteer maintainers burn out or disengage
- A significant portion of the $8.8T value is destroyed or internalised by a small number of actors.
- Software becomes more expensive, less secure or at least a smaller set of developers will scrutinise the quality.
- Innovation concentrates inside a few megacorps

Institutional Reinvention

OPEN SOURCE SecurityCon EUROPE

- Foundations evolve rapidly and take active role to support maintainers and projects
  - New legal shields for maintainers
  - Actively support projects to meet regulatory requirements

- Clear separation between code commons and deployment sovereignty
- Governments treat OSS like standards or protocols
- Growth continues (slower, but healthier)
- Trust is rebuilt at an institutional level
- Open source remains as the backbone of global software

Cultural Change

- Securing the supply chain needs developers in projects
  - Address and fix security issues and vulnerabilities
  - Support projects in adoption of tools and best practices

Typical OSPO messages… we have heard those before…

- Training of developers, managers, and decision-makers

- Open Source Contribution Processes and Policies

Need a different approach

Obligations for Manufacturers

- Exercise due diligence
- Sharing vulnerability fixes
- Effective vulnerability handling

What do they have in common?

All benefit from strong upstream collaboration

Obligations for Manufacturers

- Exercise due diligence
  - Participation provides better insight
  - Supply chain resilience through maintainer relationships

CRA compliance is less risky and costly with strong upstream engagement

  - Efficient collaboration for both project and user

- Effective vulnerability handling
  - Keep components and their dependencies to date
  - Early involvement in vulnerability response, e.g., security team participation

Do you believe me?

Need proof!

Examples and Success Stories

OPEN SOURCE SecurityCon EUROPE

- **Goal:** Upstream all security issues, no internal forks

- Work with upstream to improve security posture
  - Automated dependency management
  - Version bumps of dependencies
  - Cipher hardening
  - Adding TLS support
  - Security bug fixes
  - Exposure to public scanning tools

- Results and achievements in terms of PRs
  - 214 PRs – first level vulnerabilities
  - 1418 PRs – bumping up dependencies

Examples and Success Stories

- What did we gain
  - **Reduced maintenance burden** – Avoid private patches and feature forks
  - **Expert code review** – Get maintainers' security expertise on fixes
  - **Ecosystem-wide impact** – Your fix protects all users, not just your product

- Quick wins to start with critical projects
  - **Dependency bumps** – Submit version updates for vulnerable packages
  - **Scanner integration** – Add security scanning workflows to projects you use
  - **Documentation fixes** – Improve security configuration hardening examples

Call to Action

A network of partners with the shared goal to…

- Actively engage with upstream projects to mitigate security issues
- Create synergies and efficiency gains through mutual support and splitting of work
- Discuss mitigation of fundamental security concerns in critical projects
- Keep open source secure, interoperable, and non-fragmented

… in a safe environment (Chatham House Rule).

How about joining us?

OPEN SOURCE
SecurityCon
EUROPE

Q & A

OPEN SOURCE SecurityCon EUROPE

Co-Hosted By

CLOUD NATIVE COMPUTING FOUNDATION

OpenSSF

OPEN SOURCE SECURITY FOUNDATION