What’s in the CRA for FLOSS?

Workshop: OSS vulnerability management in light of the CRA

Christian Horchert at Huawei Cyber Security Week 2024, HCSTC Brussels

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Who am I and what is the OpenSSF?

Christian Horchert *(aka fukami)*

- works as EU Policy Advisor for OpenSSF
- redteamer most of the life at SektionEins, former ISO at EBRAINS (HBP)

OpenSSF (Open Source Security Foundation)

- is a **cross industry collaboration** of developers and security engineers within the Linux Foundation to **improve security of the open-source software ecosystem**
- publishes analysis, guidance and tools
- WGs on **various supply chain topics** (best practices, metrics, tooling, integrity, vulnerability disclosure, securing critical projects, AI/ML)

CRA Scope & Oversight

- **Connected products with digital elements** (PDE) made available on the EU market (horizontal approach)
- Applies to **all economic operators in the life cycle**: manufacturers, importers and distributors, with most obligations imposed on manufacturers
- Introduces **new economic actor**: Open Source Stewards as long-term maintainers
- **Exemptions and exclusions**, ie cars or medical devices (but not EHDS)
- In line with upcoming **product rules** including MSR and GPSR, may extends or repeals RED
- **Complemented by NIS2** (CVD, vulnerability database), **certification in CSA**
- **Market surveillance** authorities, regulatory sandboxes (incl. AI Act)

Obligations for manufacturers

- **Risk assessment**
- **Vulnerability management**, must report known vulnerabilities and incidents
- **Coordinated vulnerability disclosure** (CVD) policy mandatory
- **Support** for at least **5 years**, **security updates** for **10 years**
- Provide **Software Bill of Materials** (SBOM), but no need for publication
- **Testing** necessary, provide **technical documentation**
- **CE Marking**: must feature a CE marking **to indicate conformity** prior to entering the market, keep records for ten years

Detailed obligations and reporting duties described from Art 13 to Art 17, Art 18 lays down the obligations for authorised representatives

Obligations for importers and distributors

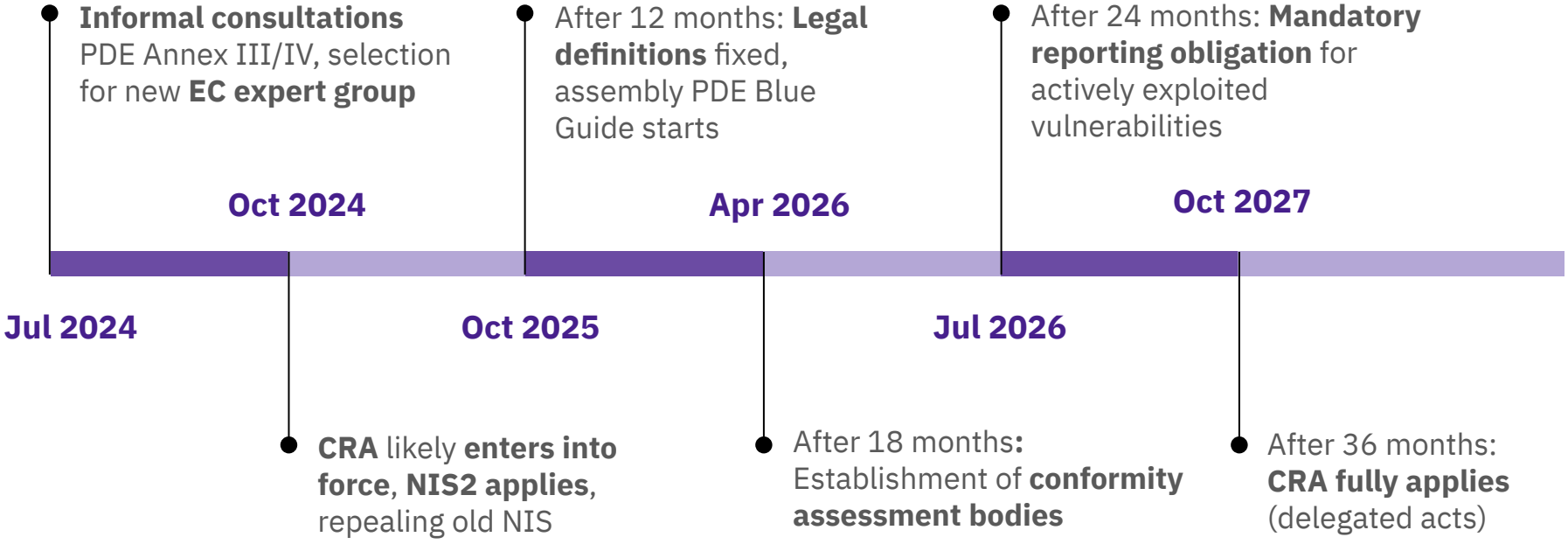
- **Due diligence**: must verify that **manufacturer demonstrates compliance**, to ensure manufacturers meet their obligations
- **Inform manufacturer of known vulnerabilities** without undue delay
- **Inform market surveillance authorities of significant risks**
- **Record retention**: Importers must retain a copy of declaration of conformity 10 years and provide it to market surveillance authorities
- **Post-product responsibilities**: Inform market surveillance authorities and users of the product (if possible) when a manufacturer has ceased operations

Obligations for importers described in Art 19, for distributors in Art 19

Open Source Stewards

- Defined in Art 2 (13) as, **legal person other than a manufacturer** with the purpose to provide sustained support **for FLOSS intended for commercial activities**
- **Obligations** are defined in Art 24:
  - **provide a cybersecurity policy** for voluntary reporting of vulnerabilities (defined in Art 15)
  - **cooperate with market surveillance authorities** and **provide documentation**
  - **report on actively exploited vulnerabilities and severe incidents** via single reporting platform (defined in Art 14)
- Stewards fall under **market surveillance rules** defined in Art 52, establishment of **ADCOs** (Administrative Cooperation Groups) to address specific questions
- Rules on **administrative fines shall not apply to Stewards**, see Art 63 (10)(2)

CRA Timeline



OpenSSF supply chain tools and projects

- **OpenSSF Scorecard**: Automated checks to **assess potential security risks** of open-source projects
- **OpenSSF Best Practices Badge**: Projects can show they follow best practices
- **Allstar**: GitHub App that continuously **monitors organizations or repositories** for adherence to security best practices
- **SLSA**: Set of **incrementally adoptable guidelines** and a way to measure efforts toward compliance to SSDF
- **Sigstore**: New standard for **signing, verifying, and protecting** software
- **GUAC**: Ingests software metadata and **maps out relationships between software**
- **OpenVEX**: Implementation of the **Vulnerability Exploitability eXchange**
- **OSV Schema**: Human and machine readable **data format** to describe vulnerabilities

How to prepare?

- **Talk to suppliers** if possible (i.e. best practises, standards used)
- **Review products and services** (especially for new developments)
- **Review existing compliance processes** (NIS2, GDPR, product specific rules)
- **Review incident response plans** and **vulnerability management processes**
- **Follow the developments** (EC, industry fora, FLOSS community…)
- **Talk to national security authorities** and other entities with similar questions
- **Take action if needed**: talk to decision makers and those that implement, they are open to feedback
- **Exercises to understand possible issues and impact** (ie. TTX offered by OpenSSF, CISA, ANSSI, ENISA)

Thank you!

Any questions?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION