EEF Security Update Q3 2025

Over the past nine months, the Erlang Ecosystem Foundation has made **important progress toward CRA readiness** for organizations that build on the Erlang Ecosystem and its rich variety of languages like Elixir and Gleam. This work reduces manufacturers' compliance burden, improves auditability, and strengthens long-term ecosystem sustainability. It is supported by community contributors and sponsors, with special thanks to **Herrmann Ultraschall** as lead sponsor.

What's already in place. The **EEF CNA** is operating to provide authoritative, machine-readable CVE data and coordinated disclosure for BEAM projects. **OpenChain certification** for Erlang and Elixir establishes recognized license and process compliance for the core runtime stack. New **package identification standards (PURLs)** make SBOMs practical and unambiguous, while **OpenVEX** enables clear, machine-readable vulnerability impact statements. Additional improvements—provenance attestations, code signing workflows, and registry integration—continue to raise the baseline.

What's coming by the end of 2025. Manufacturers will be able to consume **signed, verifiable OTP builds** (with provenance) for common targets, making conformity assessments faster and easier. **Hex.pm CVE integration** will surface vulnerability information directly where developers work, accelerating triage and due diligence. We're expanding **CNA education** so upstream maintainers handle vulnerabilities consistently, and we're establishing the Foundation as a **fiscal host**, laying the foundation for stewardship funding of critical projects.

Longer-term direction. The roadmap includes building a **stewardship model aligned with CRA Article 24**, establishing a **European entity** for regulatory alignment, setting an **SBOM baseline** across BEAM tooling, and advancing attestation-based practices in line with **CRA Article 25 and NIST SSDF**. We'll also be supporting IP protection in embedded systems (e.g., encryption/signing for `.beam` files) to reduce reverse-engineering risk while meeting integrity requirements in **CRA Annex I**.

In short, the initiative has already lowered regulatory risk for manufacturers, reduced the internal cost of compliance, and closed key gaps on the path toward CRA obligations. Continued sponsorship will preserve these gains and extend them toward long-term ecosystem sustainability.

Table of Contents

Ægis Milestones to Date

Since the launch of the Ægis initiative in early 2025, the Erlang Ecosystem Foundation has delivered several key milestones that directly advance CRA readiness and improve supply chain security across the BEAM ecosystem.

1. CNA established and operational

The EEF became a **CVE Numbering Authority (CNA)**, now ranked at the top of the CNA Enrichment Scoreboard as of September 2025, alongside organizations such as IBM and Autodesk. The CNA has already assigned CVEs, with more in progress, providing the ecosystem with authoritative and timely vulnerability data.

Impact for manufacturers & adopters: Access to machine-readable CVE metadata that integrates directly with scanners and SBOM workflows, shortening the time from vulnerability disclosure to compliance action.

2. OpenChain certification for Erlang & Elixir

Both Erlang and Elixir have achieved **OpenChain certification**, the international standard for open-source license and process compliance.

Impact for manufacturers & adopters: Ensures that the core BEAM runtimes can be used in products with digital elements while meeting license governance requirements under the CRA.

3. PURL library & new `otp` package type

The EEF Security WG implemented **PURL support** for both Hex and OTP, and built a supporting library to make PURLs easy to adopt in tooling. These new types are already in use across Erlang SBOMs, Elixir SBOMs, Mix Dependency Submission, and Mix/Rebar SBOM tooling.

Impact for manufacturers & adopters: Enables unambiguous identification of dependencies, making SBOMs accurate and actionable for audits, traceability, and regulatory reporting.

4. OpenVEX trial in Erlang/OTP

As part of the Ægis initiative, **OpenVEX** was piloted in Erlang/OTP, with contributions from Ericsson. OpenVEX provides a standard for machine-readable vulnerability impact statements, and Erlang/OTP now issues such statements for its own CVEs and vendored libraries included in the source.

Impact for manufacturers & adopters: Makes it possible to distinguish whether a deployed Erlang VM is affected, reducing false positives and unnecessary remediation work.

5. Provenance Attestations

First-level provenance attestations have been implemented for Elixir and Gleam releases, as well as for SBoM Document generated by Erlang, providing metadata about how artifacts were built and by whom. While not yet using trusted builders, this marks a key step toward reproducible, verifiable supply chains.

Impact for manufacturers & adopters: Facilitates CRA-mandated provenance documentation and supports the creation of trustworthy SBOMs.

6. Windows Code Signing

Signed binaries have been delivered for Elixir and Gleam on Windows, with work on automated delivery for Erlang in progress. Signed builds reduce the risk of tampering and improve trust in distributed artifacts.

Impact for manufacturers & adopters: Provides verifiable artifacts ready for integration into regulated build pipelines.

7. Mix Dependency Submission

Implemented across roughly 70 open-source repositories, Mix Dependency Submission provides dependency graphs directly to GitHub's advisory and security tooling. Rollout for Erlang is pending fixes on GitHub's side.

Impact for manufacturers & adopters: Improves visibility of vulnerabilities and licensing in upstream projects, supporting CRA due diligence and SBOM completeness.

8. Security Hardening of Elixir

Targeted improvements raised Elixir's **OpenSSF Scorecard rating** from 5.9 to 8.0, reflecting better practices in areas like branch protection, dependency updates, and CI/CD security. The project now carries the **OpenSSF Scorecard badge**, making its security posture visible to adopters and auditors.

Impact for manufacturers & adopters: Demonstrates adoption of recognized secure development practices, helping align with CRA Article 13 obligations around secure product development.

Near-Term Roadmap

The next phase of the Ægis initiative focuses on deliverables that provide immediate compliance and security value for manufacturers building on the BEAM ecosystem, with work progressing in the near term.

1. Signed OTP builds with provenance

Cross-platform signed OTP builds will be distributed for Linux, Windows, and macOS, covering both Intel and ARM architectures, with variations for `glibc` vs `musl`. Each build will include provenance attestations and an index file documenting its characteristics.

Impact for manufacturers & adopters: Provides trusted, verifiable artifacts that can be integrated directly into build pipelines, simplifying SBOM generation and supporting CRA requirements for provenance and update integrity.

2. Hex.pm CVE integration

Vulnerability data from the EEF CNA will be integrated into Hex.pm, the central package registry for the BEAM ecosystem.

Impact for manufacturers & adopters: Ensures vulnerabilities are surfaced at the source, giving developers and auditors immediate insight into risks and speeding up due diligence.

3. CNA education and outreach

Expanding training and resources for library authors to handle vulnerabilities consistently, aligned with responsible disclosure best practices.

Impact for manufacturers & adopters: Improves resilience of the entire supply chain by ensuring that vulnerabilities are disclosed, triaged, and remediated in predictable ways.

4. Foundation as fiscal host

The EEF will establish itself as a **fiscal host** for projects, enabling funding to flow into critical ecosystem libraries and infrastructure.

Impact for manufacturers & adopters: Creates a sustainable path for ongoing maintenance and compliance of core dependencies, reducing the risk of unsupported or non-compliant software in regulated products.

Long Term Vision

The Ægis initiative is designed not only to address immediate compliance needs but also to establish a sustainable foundation for the BEAM ecosystem over the coming years. The long-term roadmap focuses on aligning open-source projects with regulatory obligations such as the CRA, building durable stewardship structures, and advancing security practices to “state of the art” standards. For manufacturers and adopters, this ensures that the technologies they rely on remain compliant, maintained, and resilient well into the future.

1. Stewardship vessel

Establishing an Apache-style model where projects can transfer governance, intellectual property, and trademarks into the Foundation. The EEF is planning to serve as steward for **Erlang Ecosystem core libraries and projects**, ensuring baseline security and compliance standards while providing a sustainable home. This role aligns directly with **CRA Article 24**, which defines obligations for open-source software stewards, including vulnerability handling policies and cooperation with regulators.

Impact for manufacturers & adopters: Reduces the risk that critical dependencies fall into neglect or non-compliance, while ensuring there is a recognized steward able to meet CRA expectations.

2. European entity

The EEF plans to establish a European legal entity to engage directly with regulators and industry groups.

Impact for manufacturers & adopters: Creates a trusted point of contact within the EU for regulatory alignment, providing clearer guidance and reducing uncertainty around compliance obligations.

3. SBoM Baseline

Defining and delivering a **baseline level of SBOM support** across BEAM tooling, ensuring that all projects can provide essential supply chain transparency.

Impact for manufacturers & adopters: Makes it possible to consistently generate SBOMs that meet CRA expectations, simplifying audit preparation and supplier due diligence without requiring every project to implement its own approach.

4. CRA / NIST SSDF certified tooling

Bringing core infrastructure — compilers, build tools, Hex.pm, and signing services — up to standards aligned with the **NIST Secure Software Development Framework** and **certified against CRA requirements**. Much of this work builds on **attestations**, which support the framework envisioned in **CRA Article 25** on voluntary security attestation of open-source software.

Impact for manufacturers & adopters: Provides recognized evidence for conformity assessments and assurance that dependencies are developed using state-of-the-art practices.

5. Intellectual property protection in embedded systems

Work is underway with an implementation partner to introduce **encryption and signatures for `.beam` files**, ensuring that deployed software cannot easily be disassembled. The EEF will support this process through collaboration on the implementation design and by conducting independent testing and audits. This directly supports **CRA Annex I, Part I, Clause (2)(f)**, which requires protection of integrity against unauthorized manipulation or tampering.

Impact for manufacturers & adopters: Strengthens protection of proprietary applications built on Elixir/Nerves, reducing reverse-engineering risk while maintaining compliance with integrity requirements.

6. Dedicated staff growth

Expanding the initiative with dedicated full-time staff in both **security engineering** and **sponsorship/adoption**. This ensures technical delivery (e.g. signed builds, SBOM tooling, vulnerability coordination) can accelerate, while outreach and fundraising broaden the sponsor base.

Impact for manufacturers & adopters: Guarantees continuity of critical security work and spreads funding responsibility across multiple sponsors, reducing reliance on any single contributor.

7. Project funding vessel

Building the capacity to act as a **funding vessel** for ecosystem projects, including the option of becoming an **OpenCollective fiscal host**. This will make it easier for companies to direct resources to the libraries and frameworks they depend on.

Impact for manufacturers & adopters: Ensures that core dependencies remain maintained and compliant, lowering the risk of unsupported or abandoned software in regulated products.

Funding & Sustainability

The Ægis security initiative was launched thanks to the leadership of **Herrmann Ultraschall as lead sponsor**, and has since grown with contributions from **Ericsson, Dashbit, HCA**, and community volunteers. This combination of sponsorship and in-kind support has made the CISO role and all progress to date possible. Our **momentum is growing**, with more organizations joining and new opportunities for collaboration emerging.

To broaden the base of support, the Foundation is pursuing a **multi-source funding model**:

- **Foundation Sponsorship —** direct financial support from companies who rely on BEAM technologies.
- **Initiative Sponsorship —** contributions (financial or in-kind) targeted to specific deliverables such as signed builds or SBOM tooling.
- **Grants —** several applications are in progress to support audits and package security.

This approach ensures that no single company bears the responsibility alone, while still delivering concrete outcomes.

The Foundation has also begun organizing funding for **ecosystem initiatives**, such as the Expert language server and Nx, and is preparing to extend this to other projects in the future. To accelerate this work, we are expanding capacity with dedicated staff, including Daniel Janowski, who is overseeing renewed efforts in sponsorship and adoption.

Looking forward, we are preparing to:

- Establish the Foundation as a **fiscal host** for projects, allowing resources to flow directly into critical libraries and frameworks.
- Grow dedicated staff in **security engineering** and **sponsorship/adoption** to guarantee continuity of technical delivery and scale outreach to new sponsors.

Together, these steps create a sustainable path for security and compliance in the BEAM ecosystem.