FROM IDEA TO REMEDIATION IN 100 DAYS: HOW THE INDUSTRY HAS RALLIED BEHIND OSERA AND AKRITES

Discovery is now machine-speed. The patch window has collapsed.

~48,000 CVEs in 2025 — 131 a day · 78% of exploitation begins on or before disclosure day · < 5% of AI-surfaced vulnerabilities patched

THE COLLECTIVE LINUX FOUNDATION RESPONSE

UPSTREAM

Akrites

LF · June 2026 · cross-industry

- A shared security incident response team for critical open source
- One front door for maintainers: coordinated disclosure
- Maintainer of last resort

DOWNSTREAM

OSERA

FINOS · June 2026 · bank-governed

- Patch the exact versions the sector runs — fixed once, for all
- An open standard for what a patch must prove
- Signed releases through your existing proxies — zero CI change

osera

HOW OSERA HELPS FINANCIAL INSTITUTIONS GROW OSS SUPPLY CHAIN RESILIENCY

Patching is only half of the problem



OSERA — the Open Source Enterprise Resiliency Alliance. A neutral, member-governed answer to a global problem, built so enterprises of every size, in every jurisdiction, can consume it. Operational resilience without the lock-in — incubated in financial services, where the regulatory bar is highest.

Gabriele Columbro · Executive Director, FINOS · osera.finos.org

FINOS

THE LINUX FOUNDATION

OSERA is a FINOS initiative, part of the Linux Foundation

The fixes exist. Getting them to production is the hard part

In a bank, a **dependency upgrade is not a pull request**. It is a change record, a regression run, a risk acceptance and an audit trail — multiplied by thousands of applications, inside a shrinking window.

Change control & release windows

Every version bump is a change ticket with test evidence, approvals and a rollback plan. Freeze periods and release trains add weeks to a fix that took hours to write.

Regulatory evidence

DORA, NIS2 and the EU CRA expect you to prove what you fixed, when and how — with incident and change reporting on the clock. A patch with no attestation is unfinished work.

Competing priorities

Around 70% of bank IT budgets go to keeping legacy running. Backpatching a library nobody "owns" loses to every revenue project — until the CVE wave hits.

Each firm fixes it alone (or "The fork tax")

1 in 5 financial institutions have separate teams maintaining private forks of the same project or paying independently the same vendors. The same fix, re-created, re-tested and paid for many times over.

92%

of codebases carry open source components 4+ years out of date — only 7% of components in use are the latest version.

Black Duck · OSSRA 2026

6 in 10

security incidents hit where a patch already existed but had not been applied — unchanged year on year.

TuxCare · 2026 OSS Landscape · J.P. Morgan · Patchmageddon

Only 1 in 3

institutions are confident the components they consume are maintained and current. The rest are the weak links.

FINOS · The State of Open Source in Financial Services Report (2024)

"If we maintain an unmaintained library alone, it is going to cost X. If we chip in with another organization, it is going to cost half X."
Senior engineering leader, global investment bank, 2026 State of Open Source in Financial Services

IN Q1 2026 WE STARTED EXPLORING

Industry-wide prioritisation with the OSERA Risk Navigator

Our Open Source Risk Navigator turns an enterprise SBOM + vulnerability data into a practical remediation view: what is exposed, which projects are affected, and where upgrades or back patches should be prioritised. A highly interconnected industry **is only as secure as its weakest link**.

AVAILABLE TOOLING

Prioritise open source remediation with Risk Navigator

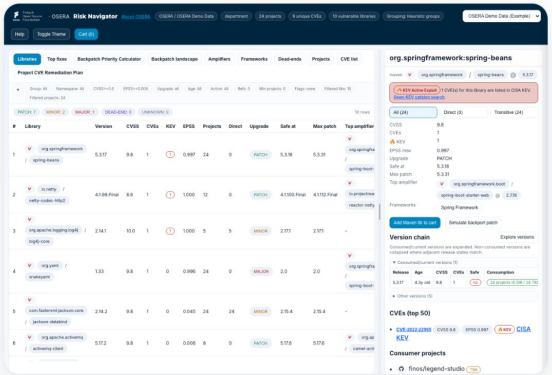
Risk Navigator turns dependency and vulnerability data into a practical remediation view: what is exposed, which projects are affected, and where upgrades or backpatches should be prioritised.

From vulnerable libraries to action

Use the overview to inspect vulnerable packages, CVEs, affected projects, safe versions, and backpatch candidates before bringing work into the OSERA formation process.

- Rank libraries by CVSS, KEV, EPSS, project footprint, and upgrade path.
- See which applications are directly or transitively exposed.
- Identify candidates for upgrade guidance, OpenRewrite recipes, or backpatch work.

Open Risk Navigator | See related workstreams



From vulnerable libraries to action

- Rank libraries by CVSS, KEV, EPSS, project footprint and upgrade path
- See which applications are directly or transitively exposed
- Identify candidates for upgrade guidance, OpenRewrite recipes or backporting work
- Track and report evolutions of your estate over time as fixes are produced

risknav.osera.finos.org

Why it matters: the backlog is demand-driven. empowering Members prioritize what matters and identify mutualization opportunities was the first order of business.

WHY NOW — PATCHMAGEDDON

AI changed one thing: how fast a known flaw gets exploited

AI has collapsed the window between disclosure and exploitation — and turned a calculated risk into a board-level exposure.

~48,000

CVEs published in 2025 — up 20.6% year on year, ~131 every day. AI-driven discovery pushes 2026 well beyond the trend.

CVE Program · J.P. Morgan analysis

0 days

average time from disclosure to first exploitation. ~78% of exploitations now begin on or before disclosure day

J.P. Morgan · Patchmageddon (2026)

~3,900

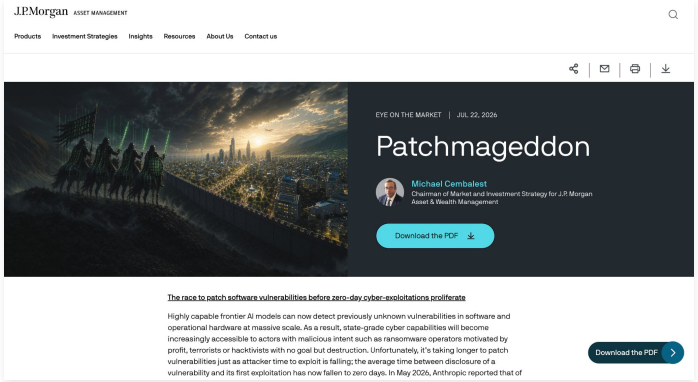
high & critical open source vulnerabilities surfaced by a single Mythos-class model preview. Discovery is now machine-speed.

Anthropic disclosure, May 2026 · via Patchmageddon

66

CVEs in a single month on one framework family (Spring, June 2026). CVE waves — not single CVEs — are the new operating condition.

Spring security advisories, June 2026



WHAT CHANGED FOR THE C-SUITE

Yesterday an accepted, tolerated backlog of known-but-unpatched versions.

Today a top C-level priority — boards and regulators want evidence, not intent.

Long term vision consuming fixes at scale from upstream and from commercial patch vendors needs structure: one standard, one gate, many producers.

OUR INTENT TO FORM IN JUNE 2026 — OPERATIONAL RESILIENCE, WITHOUT THE LOCK-IN

Public source. FSI-grade releases. No single choke-point

We apply fixes for known CVEs to the exact projects and versions the sector still runs — prioritised across firms, produced by vendor maintainers under an alliance SLA and contract and accepted only through the Remediation Standards gate.

1 KNOWN CVE IN A [PACKAGE, VERSION]

Surfaced and prioritised across firms

→

2 FIX PRODUCED & TESTED

By vetted vendor maintainers under an alliance SLA and open under the upstream license — green CI on the upstream test suite, through the **Remediation standards** acceptance gate.

→

3 FSI-GRADE RELEASE

Signed builds with standard based attestations pulled from FINOS hosted artifact repositories through your existing proxy with the coordinates you already use. Zero CI change.

SOVEREIGN BY DESIGN — WHY THIS MATTERS IN EUROPE

Neutral venue

Linux Foundation / FINOS governance, one firm one vote. No single vendor and no single country controls it.

No lock-in

Every backport is open source — mandatory. Leave any time and keep the source; forks are portable. No commercial EOL cliff.

A two pronged platform built to scale

OSERA's vision is to build a platform that directly connects the demand of financial institutions - and other enterprises - to the open source supply side, creating frictionless opportunities for vendors and maintainers

No jurisdictional chokepoint

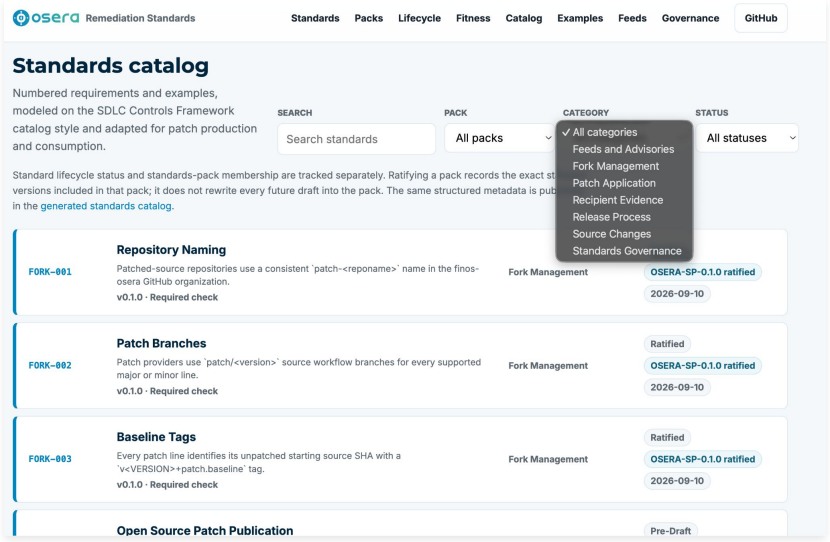
Removing vendor lock-in also removes the dependency on one supplier's jurisdiction — or export decision — to consume what you already run. Strong global banks representation: a global answer to a dependency that is global by nature.

Releases are meant to be time-bound — a managed bridge to a current, supported version, not a licence to stay behind. Source public, built artifacts member-only.

OPEN STANDARD · STANDARDS.OSERA.FINOS.ORG

Remediation Standards: what a patch must prove, for everyone

The first wave of patched projects matters. **The agreement on how any fix must be produced, verified and attested matters more** — it is what lets the sector consume at scale from upstream and from many producers.



v0.1 published · Community Specification License

WHY THIS MATTERS ABOVE AND BYOND OSERA

One acceptance gate

Any package from any producer enters OSERA repositories only if it complies — the same bar no matter who produced the fix.

Commercial patch producers

Comply once, ship into every member bank. The standard replaces per-bank due diligence with shared, verifiable evidence.

SCA & supply-chain vendors

One industry-wide lingua franca for patches and attestations — SBOM, VEX, provenance, signing — to build products against.

Read the standard

"An open, verifiable standard for remediation delivers trust at scale — especially critical as the industry consumes open source from the community and from multiple patch vendors and coalitions."

Dov Katz · MD & Distinguished Engineer, Morgan Stanley · Chair, OSERA Remediation Standards WG

JUST A MONTH AGO · 100 DAYS IN

100 days in: banks back industry-wide standards and fixes

6

Premier members: Citi, Deutsche Bank, Goldman Sachs, Morgan Stanley, NatWest, RBC. Three of six outside the US.

3 weeks

to publish v0.1 of the open Remediation Standard — banks, patch producers and infra leaders, together.

50+

widely used Spring & Java projects patched with standard attestations — ready for production use by members today.

0

CI changes: bank pilots pulled hardened releases through existing corporate proxies, same coordinates.

Read the release

What's Next:

- ≥ 80 patches a month under SLA - more Java and coverage across ecosystems
- first end-to-end OSERA platform release at OSFF New York, 4–5 Nov
- per-project sponsorship model
- remediation-standards

PREMIER MEMBERS

citi · Deutsche Bank · Goldman Sachs · Morgan Stanley · NatWest · RBC

PARTNERS & CONTRIBUTING VENDORS

Moderne (creators of OpenRewrite) · controlplane · sonatype · Scott Logic

JOINED FINOS SINCE OSERA LAUNCHED

Chainguard · docker · herodevs · RAPIDFORT

ANNOUNCEMENT: THE OSERA EXCHANGE IS OPERATIONAL

1 Secure intake

oseractl — anonymized [package, version] only

2 Cross-firm prioritization

Risk Navigator — demand-driven backlog

3 Fix produced & tested

Vetted vendor maintainers under SLA — green CI on the upstream suite

4 FSI-grade release

Signed builds with VEX and test evidence, through your existing proxy

PREMIER MEMBERS

citi · Deutsche Bank · Goldman Sachs · Morgan Stanley · NatWest · RBC

+ 3x new Premier members announced in the next few weeks

THE MEMBER VENDOR ECOSYSTEM PARTICIPATING IN OSERA

Moderne — The agent tools company · controlplane · sonatype · Scott Logic · Chainguard · RAPIDFORT · herodevs

HOW IT WORKS: CONFIDENTIALITY BY DESIGN

Only [package, version] ever leaves the bank — no SBOMs, no usage data, no volumes, no firm attribution

INSIDE THE BANK	THE ALLIANCE — FIXED ONCE, FOR ALL	BACK INSIDE THE BANK
1 Detect — Scanners flag a dependency, or a new CVE lands on a maintained line	**3 Dedupe & score** — Risk Navigator: severity × reach × cross-firm overlap	**6 Consume** — Through your existing proxy: one coordinate change, zero CI change
2 Request — File the [package, version] tuple with oseractl	**4 Produce & gate** — A vetted vendor maintainer builds it; conformance tests enforce the Standard	**7 Evidence** — Attestation pack for risk and audit — DORA, NIS2, CRA
	5 Publish — Signed artifact + SBOM, VEX, provenance to the member repository	

Fixed once, for all: public source · member-only attested releases · time-bound by design — a bridge to a current version, not a licence to stay behind

LIVE FROM OSERA.FINOS.ORG

420

libraries with hardened releases

4,610

patched entries — CVE × artifact version

78

libraries with at least one fixed CVE

130

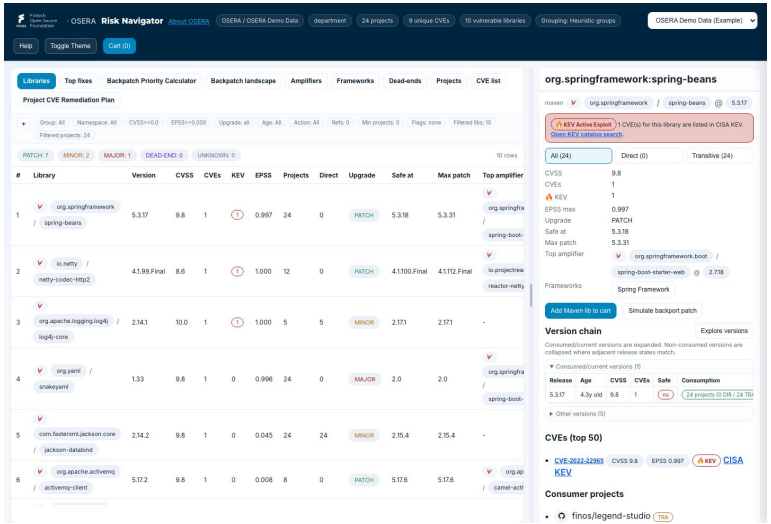
releases in a single day — Oct 23

13

ratified Remediation Standards

0

CI changes to consume any of it



Risk Navigator
CVSS · KEV · EPSS · footprint · cross-firm overlap · upgrade path

SUPPORTED ECOSYSTEMS:
JAVA AND JAVASCRIPT

GET INVOLVED

Built in finance. Open to every enterprise and every producer

Incubated where the regulatory bar is highest — open to institutions of every size, to any enterprise with the same dependency, and to technology firms with upstream expertise, anywhere in the world. **Help us shape what's next!**

FOR END USERS

Financial institutions — and any enterprise

Fund and govern the alliance, or consume FSI-grade releases at your scale with General-tier fees sized for smaller firms. The need is not unique to finance: where the demand is, this grows beyond FINOS.

Become an OSERA member →

osera.finos.org/#involved

FOR VENDOR MAINTAINERS

Upstream expertise, under an SLA

Put your maintainer credentials under an OSERA SLA: join the workstreams, shape standards, work for one of the most sought after industries without procurement headaches.
Open to every FINOS member — no OSERA membership required.

Become a FINOS member →

finos.org/become-a-member

FOR PATCH & SCA VENDORS

Comply once, sell everywhere

Commercial patch producers and SCA / registry vendors adopt the Remediation Standards to cut go-to-market friction into FSI — one attestation format every member bank accepts.

Join the Standards WG →

standards.osera.finos.org

Everyone can build it from source — **github.com/finos-osera-forks** · Supported lines and the standards, in one document: **the OSERA Prospectus →**

AKRITES + OSERA

Fix it once, for everyone — and prove it.

Now the practitioners: Dov Katz, Morgan Stanley · Peter Thomas, Deutsche Bank · Brian Fox, Sonatype & Chair of Akrites — moderated by Tosha Ellison

osera