A FINOS INITIATIVE · PART OF THE LINUX FOUNDATION · PROSPECTUS

OSERA Open Source Enterprise Resiliency Alliance

Secure open source. In production. At scale.

Published-data snapshot
30 October 2026
Live figures: osera.finos.org

For CISOs, application security, platform engineering and open source risk leaders at regulated institutions, and for the technology firms that serve them.

WHAT IT IS

Regulated institutions run much of the same open source, often on versions upstream no longer patches, and each pays separately to secure it: forking, patching in-house, or buying private support for the same CVEs. **OSERA replaces that fork tax with one openly governed programme.** Known CVEs are fixed once, in the exact projects and versions the sector still runs in production, by vetted vendor maintainers under an alliance SLA, and every release is accepted only once it clears the **OSERA Remediation Standards**. Patched source stays public; members take signed, packaged releases with SBOMs, VEX and test evidence through their existing proxy, with no CI change. Operational since August 2026.

7 members Members include citi · Morgan Stanley · NatWest · RBC

PUBLISHED REMEDIATION AT A GLANCE

Delivered, attested fixes only · official feeds as of 30 October 2026, 08:18 UTC

216	4,610	78	21	495
Distinct CVEs addressed	**Patched entries**	**Libraries with fixes**	**Upstream projects**	**Published release sets**
Unique CVE identifiers with a published fix	CVE × artifact version: one fixed CVE on one exact build	Of 420 library coordinates in published releases	With at least one published fix (Java)	Promoted as whole sets

Patched entries count CVE × artifact-version pairs, not unique vulnerabilities. Distinct CVEs exclude 2 GHSA-only advisories. Sources: **feed.finos.org/stats/metrics.json** (as of 30 October 2026, 08:18 UTC) and **feed.finos.org/openvex.json** (OpenVEX v160, last updated 30 October 2026, 08:18 UTC). Backlog and candidate lines are counted separately and are not included here.

HOW IT WORKS

1 Members submit [package, version]
Through a secure intake, prepared in Risk Navigator. A project and a version, not a CVE list and never an SBOM. The public backlog carries no firm attribution.

2 Automated prioritization
One neutral score: severity, known exploitation (KEV), exploit likelihood (EPSS) and anonymized member demand. A shared dependency is patched once.

3 Public fork, upstream first
Approved vendor maintainers fix the project in public under **finos-osera-forks**, and offer the fix back wherever upstream is alive.

4 Member release
Only Standards-compliant packages are promoted. Green CI on the upstream test suite; consumed through your existing proxy and coordinates.

WHY IT MATTERS

Patch once, consume everywhere.
216 CVEs fixed once, consumed by every member.
Each fix replaces remediation every institution was producing privately. One in five financial services firms has separate teams maintaining forks of the same project (FINOS, 2025).

No CI change.
Change a version coordinate. Keep your pipeline.
For a large project such as Spring, the maintained BOM carries the patched versions, so one BOM update covers the line. Scanners read the published VEX and show the CVE resolved on that exact build.

Audit evidence, not assurances.
Signing, SBOMs, VEX and tests on every release.
Evidence mapped to the Remediation Standards, built for DORA and NIS2 supervision today and the EU CRA: reporting duties from September 2026, full vulnerability handling from December 2027.

Fixes at the speed of exploitation.
Pooled, pre-tested fixes, not one queue per firm.
About 78% of exploitations now begin on or before CVE disclosure day, up from 19% in 2018 (J.P. Morgan, 2026). Priced from $15k so institutions of every size and jurisdiction take the same fix.

WHO'S BEHIND IT

Governed by the institutions that run the software, under FINOS neutral governance: one firm, one vote, so no single vendor or country controls the fix. The board sets policy; backlog ordering is automated on neutral scoring. Standards WG chair: Dov Katz, Morgan Stanley.

Built with expert vendors: Moderne (vendor maintainer), Sonatype (supply-chain infrastructure), ControlPlane (security engineering), Scott Logic (community support). Complementary to the Linux Foundation's Akrites, which coordinates the upstream response; OSERA operationalizes it downstream.

PUBLISHED COVERAGE BY UPSTREAM PROJECT

All 21 projects with a published fix · as of 30 October 2026

PROJECT	MAINTAINED VERSION LINES WITH FIXES	LIBRARIES	DISTINCT CVES	ENTRIES
Spring	Boot 2.7 · Framework 5.3 · Security 5.7 · Data 2.7/3.4/3.7 · GraphQL 1.0 · HATEOAS 1.5 · Integration 5.5 · Kafka 2.8 · LDAP 2.4 · WS 3.1	33	63	931
Bouncy Castle	1.46 · 1.69 · 1.70 · 1.78	8	51	2,586
Jackson	2.13 · 2.15 · 2.19	4	23	540
Eclipse Jetty	9.2 · 9.4	10	17	165
Apache Log4j	1.2 · 2.17 · 2.24	4	14	53
SnakeYAML	1.9 – 1.33 (11 lines)	1	7	228

Also fixed: lz4-java 1.8 (7) · Apache Struts 1.3 (6) · Apache Xerces 2.2 (4) · c3p0 0.2/0.9 (4) · Apache Axis 1.4 (4) · Logback 1.2 (3) · Commons BeanUtils 1.6/1.8/1.9 (2) · dom4j 1.4 (2) · Reactor Netty 1.0 (2) · HttpComponents 5.3 (2) · Commons Text 1.6/1.7/1.8/1.9 (1) · Commons Configuration 1.1/1.9 (1) · Apache Velocity 1.6/1.7 (1) · Commons Collections 3.0 (1) · Hibernate 5.6 (1)

Figures in brackets are distinct CVEs. Lines are major.minor versions carrying at least one published fix; Spring is shown by sub-project. Projects are grouped by Maven group ID. Search every artifact, version and CVE in the live catalog at **osera.finos.org/how-it-works#search**.

Delivered

Published, Standards-gated releases only: the figures on this page and page 1. Live and growing as new ecosystems and lines are released.

- Live catalog: osera.finos.org/how-it-works
- Live stats: feed.finos.org/stats

Backlog: not yet delivered

Lines piloted before launch and new member [package, version] submissions, ranked in Risk Navigator by CVSS, KEV, EPSS, footprint and cross-firm overlap. Tracked publicly, never counted as delivered.

- CVE backlog: github.com/finos-osera-forks/backlog
- Next: further ecosystems beyond Java

REMEDIATION STANDARDS

OSERA-SP-0.1.0 · ratified 10 September 2026 · 13 ratified, 7 observe-only

Every OSERA release, whether upstream contribution, public fork or signed member artifact, is accepted only once it clears the Standards: a shared bar institutions can also apply to fixes from upstream and commercial producers.

Release Process — 6 + 3 observe
Version naming, approved producers, test provenance, bytecode compatibility, hygiene.

Fork Management — 3 + 1 observe
How patched-source repos, patch branches and baseline tags are named and published.

Source Changes — 2 + 1 observe
Upstream provenance links for every backport; licence headers on new files.

Feeds & Advisories — 1 ratified
OpenVEX and CycloneDX feeds, so a release states what it fixes and scanners can read it.

Recipient Evidence — observe
What changed and what to test, as evidence for auditors and regulators.

Patch Application — observe
How a patch feed is discovered and applied across a dependency estate.

Plus STD-001, standards-as-code governance. Version 0.2.0, with the next attestations, is planned for end of 2026. Full text: **standards.osera.finos.org**.

ROADMAP: FROM FIRST RELEASES TO AN OPEN PRODUCER MARKETPLACE

FORMATION
Jun – Aug 2026
Intent announced 26 June. Operational in August: Premier members sign, Board convenes.

STARTUP
10 Sep 2026
Remediation Standards pack 0.1.0 ratified, five weeks after going operational.

DELIVERING NOW
Oct 2026
Java live. 216 CVEs addressed across 21 upstream projects and 495 release sets by 30 October.

NEXT
End of 2026
Per-project sponsorship, further ecosystems, Standards 0.2.0 with the next attestations.

SCALING
2027 and beyond
Multiple producers, full exchange model, bring-your-own maintainer, AI-driven remediation.

ENGAGEMENT OPTIONS

1 $100,000 / year

Premier member. Fund and govern: approve and sunset projects, maintenance scope, SLAs and vendor-maintainer bids; Governing Board and committee seats, one firm one vote; member-only releases.

2 $15,000–$90,000

General member, by firm size. The same attested releases, the right to propose projects, working groups; one board and committee seat for the class.

3 No OSERA fee

FINOS member. Join the Standards and Risk Navigator workstreams and bid to become a vendor maintainer. Patch and infrastructure vendors conform through FINOS.

4 Open source

Build it yourself. Every maintained line is public under the upstream licence at github.com/finos-osera-forks; fixes are offered back to receptive upstreams.

GET INVOLVED

Join: enrollment.lfx.linuxfoundation.org/?project=osera · compare tiers at osera.finos.org/alliance#membership · not yet a FINOS member? membership@finos.org

See what is fixed today: osera.finos.org/how-it-works#search · feed.finos.org/stats · forks at github.com/finos-osera-forks

Read the standards at standards.osera.finos.org · **propose a project or bid to maintain one:** osera.finos.org/#involved