RL Blog | ReversingLabs

Published: 2026-04-02 · Archived: 2026-04-05 12:49:19 UTC


axios

April 2, 2026

Axios: How AppSec teams should respond

Here's a mitigations checklist and best practices. Plus: How RL’s xBOM and Spectra Assure Community can help.

Axios: How AppSec teams should respond


Software trust debt

April 1, 2026

How JPMC tackles software ‘trust debt’

JPMorgan Chase CISO Patrick Opet discussed his letter on third-party software risk — and how that has played out.

How JPMC tackles software ‘trust debt’


AI ramps up risk

March 31, 2026

GenAI Security Project ramps up guidance

With AI ramping up risk, OWASP stepped up its project to help AppSec teams get up to speed — and take action.

GenAI Security Project ramps up guidance


Cascading supply chain attack

March 27, 2026

AppSec as attacker: Inside Trivy–LiteLLM

The perimeter isn't your firewall — it's your CI/CD pipeline. Here’s what to know about TeamPCP's supply chain attack.

AppSec as attacker: Inside Trivy–LiteLLM


TeamPCP supply chain attack

March 27, 2026

The TeamPCP supply chain attack evolves

The malicious campaign started with Trivy and Checkmarx and has shifted to LiteLLM — and now telnix. Here's how.

The TeamPCP supply chain attack evolves

March 26, 2026

Decouple SIEM data to reshape your AppSec

Shift to a data security pipeline platform to get software visibility that modern supply chain threats demand.

Decouple SIEM data to reshape your AppSec

March 25, 2026

How AI agents can weaponize IDEs

Research shows that AI coding can tap integrated development environments to become privileged insider threats.

How AI agents can weaponize IDEs

March 18, 2026

OpenClaw lesson: AI agents are a black hole

AI agents create novel attack surfaces and control issues that require rethinking assumptions — and AppSec tooling.

OpenClaw lesson: AI agents are a black hole

March 12, 2026

Make Your SBOMs Actionable with PURLs

Learn how Package URLs improve vulnerability matching, which reduces alert fatigue and simplifies compliance.

Make Your SBOMs Actionable with PURLs

March 11, 2026

OWASP adopts DockSec: Why it matters

OWASP has adopted the container security tool to slow information overload. Here’s what you need to know.

OWASP adopts DockSec: Why it matters

March 10, 2026

OpenClaw and AI risk: 3 AppSec lessons

The OpenClaw saga is a case study on the threat from agentic AI, showing how it increases software risk.

OpenClaw and AI risk: 3 AppSec lessons
