NEWS RELEASE

JFrog Closes the Patching Gap with Universal Zero-Touch Remediation, Bringing Leading Patching Vendors into One Source of Truth

2026-11-03

JFrog Builds a Self-healing Software Supply Chain with Broadcom, Chainguard, Echo, and Red Hat and others to answer the AI-era demand for remediation in hours

SUNNYVALE, Calif.--(BUSINESS WIRE)-- JFrog Ltd. (“JFrog”) (NASDAQ: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, the system of record for trusted software artifacts, binaries, and AI assets, today shared insights from a swampUP Europe security expert panel in which leaders from Broadcom, Chainguard, Echo, and Red Hat confronted a shared problem: *“the patching gap”*. Their unanimous conclusion: organizations can no longer rely on manual vulnerability triage and patching. Resilience in the AI era depends on three key elements: a single source of truth where every artifact lives; an ecosystem of patching vendors producing fixes faster than disclosure; and a self-healing software supply chain that enables continuous, zero-touch remediation at the speed of the threat.

JFrog Builds a Self-healing Software Supply Chain with Broadcom, Chainguard, Echo, and Red Hat and others to answer the AI-era demand for remediation in hours

“Having a single source of truth is essential for protection in today’s AI threat landscape, but visibility is only part of the problem. It’s also an issue of speed and a shift in the type of weakness itself,” said Nico Thirion, Field CISO, JFrog. “Attackers today chain together low-severity findings and run thousands of automated attempts until one unpatched system gives them an opening. This is a different kind of challenge needing a different approach. JFrog has adapted to this new requirement by focusing on early detection, accurate determination of exposure, and zero-touch

remediation that enables customers to patch in hours vs. days."

Rebuilding the Disclosure and Remediation Process for the AI Era

The panelists agreed there is a fundamental shift reshaping the today's security market: the decades-old vulnerability disclosure process – designed around human review cycles – wasn't built for an AI-powered world where exploitation can be automated at scale. Historically, enterprises have depended on upstream maintainers to publish patches on their own timeline – rarely in sync with the common vulnerabilities and exposures (CVE) disclosure window. With the AI surge, this traditional approach has created a new exposure gap for attackers. Consequently, a new ecosystem of patching vendors has committed to closing that gap – producing clean, signed, backported fixes at the exact versions enterprises consume, often ahead of public disclosure.

But a patch sitting in a vendor's repository does not help an artifact already running in production. This is where The JFrog Platform comes in: With JFrog Artifactory as the **single source of truth** where every artifact lives – binaries, containers, AI models, MCP servers, etc. – it acts as the control plane that ingests each partner's fix. JFrog Security automatically applies the best fix according to the customer's policy and produces a signed evidence chain that auditors can verify. The result is a self-healing software supply chain.

"Frontier AI is introducing a new security risk for every enterprise – dramatically shrinking the time between vulnerability discovery and exploitation. Traditional patching processes simply cannot keep pace with AI-powered autonomous adversaries, leaving many enterprises exposed," said Gal Marder, Chief Strategy Officer, JFrog. "Eliminating this risk requires two critical capabilities: high-quality patches across software ecosystems and a universal control plane that automates remediation at the binary level. Through our collaborations with Broadcom, Chainguard, Echo, Red Hat, and other leading patch providers, we enable organizations to eliminate the risks associated with slow, manual patching by moving toward fully automated, zero-touch remediation across their software supply chains."

Three Parts of the Industry, Converging on One Architecture

Fixing this AI-era challenge requires two parallel shifts: redesigning how vulnerabilities are disclosed and triaged, and scaling patching itself into an automated, continuous process rather than a manual, ticket-driven one. The panelists represented a cross-section of the new open-source patching economy – each taking a different angle: backporting fixes to the versions customers already run; patching end-of-life packages that upstream maintainers have abandoned; and releasing CVE-only isolated patches ahead of public disclosure.

"There's a real tension in how the industry patches open source today. Every cloud, vendor, and security team is quietly forking the same critical dependencies with its own patch set, held behind their own paywall," said Alex Burrage, Director of Product Security, Chainguard. "Left alone, the default outcome is a two-tiered internet – one where enterprises get security fixes before the maintainers who wrote the code even see them. The only way out is a shared layer where every fix is visible, verifiable, and portable."

"For over three decades, Red Hat has backported security patches across thousands of packages. Lightwell scales this exact model to meet the AI-era urgency," said David Szegedi, Chief Architect, Red Hat. "We are applying the same discipline, upstream commitment, and engineering rigor across the application layer."

The one thing all these players share is a model that produces clean, verified fixes faster than the

traditional disclosure cycle allows. All are integrated with the JFrog Self-Healing Software Supply Chain through the Zero-Touch Remediation partner network introduced earlier this year. JFrog Artifactory sits at the center of this model, serving as the single source of truth. Around it, JFrog Xray and JFrog Curation document what enters the pipeline, JFrog Zero-Touch Remediation applies fixes from the partner network at machine speed, and JFrog AppTrust attaches signed evidence that supports compliance teams attest to frameworks such as the EU's DORA and Cyber Resilience Act, without a spreadsheet or a manual audit cycle.

"TrueSource Spring Enterprise sits at the center of enterprise Java, which makes it a prime target the moment a new exploitation technique appears," said Oren Penso, Member of Technical Staff, Tanzu Division, Broadcom. "Our job is to get a verified, backward-compatible fix into a developer's hands before an automated attacker can weaponize the gap. Connecting that fix directly into JFrog's artifact workflow means teams get Broadcom's patch and JFrog's evidence chain in the same motion, without slowing down a release to do it."

"AI has changed both the scale of software development and the speed of threats. We can't keep asking security teams to manually triage every vulnerability or developers to spend hours updating dependencies," said Eylam Milner, Co-Founder and CTO, Echo.ai. "We need to start with secure-by-default components and automate the patching work, so people can focus on the judgment and engineering that need their attention."

Self-Healing Starts with a Universal Single Source of Truth

The panel's framing echoes the five pillars of JFrog's self-healing software supply chain introduced alongside JFrog Zero-Touch Remediation earlier this year. Interested customers can learn more about JFrog's Self-healing Software Supply Chain and its growing partner network by visiting https://jfrog.com/zero-touch-remediation/. More information on JFrog AppTrust and the entire JFrog Software Supply Chain Platform is available at https://jfrog.com.

Like this Story? Share this on X: *The exploit window used to be weeks. Now it's hours. At #swampUP Europe, @JFrog, @Broadcom, @Chainguard_dev, @Follow_our_Echo, and @RedHat agreed: organizations can no longer rely on manual vulnerability triage and patching, and you can't patch what you cannot see. Resilience in the #AI era starts with a single source of truth. Learn more: https://bit.ly/4eNZ0v3 #DevSecOps #DevGovOps*

About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the universal DevOps, DevSecOps, DevGovOps, and AI Security platform, is on a mission to create a world of trusted software delivery without friction from development to production, whether software is written by developers or by AI. Driven by this "Liquid Software" vision, the JFrog Platform is the software supply chain system of record for the AI era, built to help organizations manage, secure, govern, and distribute trusted software, alongside models, agents, and AI-generated assets that increasingly power it, with speed and at scale. The universal, hybrid, multi-cloud JFrog Platform is available as a managed SaaS service across major cloud providers, as well as self-managed instances. Millions of users and thousands of organizations worldwide, including a majority of the Fortune 100, depend on JFrog as a single source of truth to securely adopt AI and accelerate business transformation. Learn more at https://jfrog.com or follow us on X @JFrog.

Media Contact:
Siobhan Lyons, Director, Global Communications, siobhanL@jfrog.com

Investor Contact:
investors@jfrog.com

Source: JFrog Ltd.