JFrog Enables Trusted AI - Uncovers Critical Security Threats Emerging from AI's Expansion in the Software Supply Chain

The Software Supply Chain State of the Union 2025 Report Reveals "Quad-fecta" of Security Exploits, Mis-scored CVEs, Poor ML Model Governance, & more are Jeopardizing Trust in Newly Created Software

Sunnyvale, Calif. and LONDON (KubeCon + CloudNativeCon Europe) — April 1, 2025 — JFrog Ltd (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today released the Software Supply Chain State of the Union 2025 report, which highlights emerging software security threats, evolving DevOps risks and best practices, and potentially explosive security concerns in the AI era.

"Many organizations are enthusiastically embracing public ML models to drive rapid innovation, demonstrating a strong commitment to leveraging AI for growth. However, over a third still rely on manual efforts to manage access to secure, approved models, which can lead to potential oversights," said Yoav Landman, CTO and Co-Founder, JFrog. "AI adoption will only grow more rapidly. Thus, in order for organizations to thrive in today's AI era they should automate their toolchains and governance processes with AI-ready solutions, ensuring they remain both secure and agile while maximizing their innovative potential."

Managing and securing the software supply chain end-to-end is an imperative for delivering trusted software releases. By combining insights from over 1,400 development, security and operations professionals across the U.S., U.K., France, Germany, India and Israel, with developer usage data from JFrog's 7K+ customers, alongside original CVE analysis by the JFrog Security Research team, the JFrog Software Supply Chain State of the Union 2025 report reveals why this task is often challenging for companies amidst the expanding and frenzied threat landscape faced in today's AI era.

Key Report Findings Include:

- **A "Quad-fecta" of Security Vulnerabilities are Threatening the Software Supply Chain**: The top security factors impacting the integrity and safety of the software supply chain include: CVEs, malicious packages, secrets' exposures, and misconfigurations/human errors. As an example, the JFrog Security Research Team detected 25,229 exposed secrets/tokens in public registries (up 64% YoY). The

increasing complexity of software security threats are making it harder to maintain consistent software supply chain security.

- **AI/ML Model Proliferation and Attacks are Growing:** In 2024, more than 1 million new ML models were added to Hugging Face, with an accompanying 6.5x increase in malicious models, indicating AI and ML models are increasingly becoming a preferred attack vector for bad actors.
- **Manual Governance of ML Models is Increasing Risk:** Most companies (94%) are using certified lists to govern ML artifact usage, however over one-third (37%) of those rely on manual efforts to curate and maintain their lists of approved ML models. This overreliance on manual validation creates uncertainty around the accuracy and consistency of ML model security.
- **Limited Security Scanning Leaving Blind Spots:** Alarmingly, only 43% of IT professionals say their organization applies security scans at both the code and binary levels, leaving many organizations vulnerable to security threats only detectable at the binary level. This is down from 56% last year - a sign that teams still have huge blind spots when it comes to identifying and preventing software risk as early as possible.
- **Critical Vulnerabilities Continue to Rise and be Mis-scored:** In 2024, security researchers disclosed over 33K new CVEs, a 27% increase from 2023, surpassing the 24.5% growth rate of new software packages. This trend raises concerns as the growing number of CVEs increases complexity and pressure on developers and security teams, potentially hindering innovation. Meanwhile, JFrog Security found that only 12% of high-profile CVEs rated "critical" (CVSS 9.0-10.0) by government organizations justify the critical severity level they were assigned because they are likely to be exploited by attackers.[1] This pattern is troubling due to a centralized and unchanged scoring methodology over time, which heightens the risk of false positives in assessments and contributes to developers experiencing "vulnerability fatigue."

“We uncovered a clear pattern by CVE scoring organizations to inflate scores and cause an unnecessary level of panic in the industry, sending developers scrambling on remediation efforts that often results in wasted cognitive and professional time,” said Shachar Menashe, Vice President of Security Research. “When DevSecOps teams are forced to remediate vulnerabilities that aren’t ultimately harmful, their everyday workflows are disrupted, which can lead to developer burnout and costly mistakes.”

---

[1] *The JFrog Severity Rating methodology considers the likelihood of vulnerability exploitability, unlike CVSS ratings, which focus only on exploitation severity, often overestimating risks.*

The JFrog Software Supply Chain State of the Union 2025 report also outlines concerns around lack of code provenance visibility across the software supply chain, developers downloading open source software packages directly from public registries without filtering for vulnerabilities, the detriments of "security tool sprawl", and more. To explore the full findings of this year's report visit https://jfrog.com/software-supply-chain-state-of-union/ or read this blog.

You can also register to join JFrog security and developer experts on Thursday, April 24, 2025 at 9 AM PT for a webinar, "JFrog's Software Supply Chain Report 2025: Trends, Threats & Actions," detailing the challenges and complexities of managing and securing the software supply chain.

###

Like this Story? Share this on X (a.k.a. Twitter): @JFrog shares research findings in their Software Supply Chain State of the Union 2025 report. Discover the emerging #DevSecOps trends, risks & best practices to securing enterprise #SoftwareSupplyChain. Learn more: https://jfrog.co/43vkg3Y #SoftwareSupplyChain #DevOps #DevSecOps #cybersecurity #containers #CVE

About JFrog

JFrog Ltd. (Nasdaq: FROG) is on a mission to power the world with liquid software. We are replacing endless software updates with a single system of record that seamlessly delivers secure applications from developer to device. The JFrog Software Supply Chain Platform helps organizations build, manage, and distribute software quickly and securely, making applications available, traceable, and tamper-proof. Its integrated security features also help identify, protect, and remediate against threats and vulnerabilities. The Platform also brings ML models in line with all other software development processes, providing a single source of truth for all software components across Engineering, MLOps, DevOps, and DevSecOps teams so they can build and release AI applications faster, with minimal risk and less cost. JFrog's hybrid, universal, multi-cloud platform is available as both self-hosted and SaaS services across major cloud service providers. Millions of users and 7K+ customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation. Once you leap forward, you won't go back! Learn more at jfrog.com and follow us on X: @jfrog.

Media Contact:

Siobhan Lyons, Sr. Manager, Global Communications, siobhanL@jfrog.com

Investor Contact:

Jeff Schreiner, VP of Investor Relations, jeffS@jfrog.com