New JFrog Report Warns: AI Governance Fails as Software Supply Chain Attacks Hit Record Highs

The Hidden Costs of AI at Scale: JFrog's 2026 Software Supply Chain Security report shows threat actors weaponizing developer workflows, driving 177K new malicious packages, 495 malicious AI models, and a 451% increase in infected npm packages

SUNNYVALE, Calif. – May 20, 2026 – JFrog Ltd. (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 announced the findings of its **2026 Software Supply Chain Security State of the Union** report. This year's report reveals an unprecedented acceleration in enterprise software risk as threat actors expand strikes beyond traditional package registries into AI model registries and developer tooling, creating a blind spot in current software governance frameworks.

"Every enterprise is adding AI to their software supply chain, which is increasing the attack surface for bad actors. Our report shows attackers are no longer just breaching traditional defenses – they are actively weaponizing the trusted models, registries, and agentic tools driving today's AI-powered development. The era of 'scan and hope' is over," said Shlomi Ben Haim, CEO & Co-Founder, JFrog. "Organizations need a single source of truth that governs every binary, every model, and every AI agent skill from the moment it enters the pipeline to the moment it is deployed in production. This is what JFrog was built to deliver."

As AI moves from experimentation to a structural force reshaping the software supply chain, organizations are seeing a widening gap between reported security confidence and the risks accumulating in their infrastructure. Drawing on data from 18.2 billion artifacts managed across the JFrog Platform (up 136% year-over-year), original vulnerability research by the JFrog Security Research team, and a global survey of 1,508 security and DevOps professionals [1], this report exposes what it calls the "illusion of mastery", i.e. the growing disparity between perceived security and the reality of mounting supply chain risk.

Key Findings Include:

- **Malicious Packages Hit an All-Time High:** Malicious npm packages surged 451% year-over-year, with 177K new malicious packages detected across registries in the last year. Attackers are exploiting trust at scale – the "Qix" campaign used just 25 packages to compromise over 2.5 million downloads.
- **AI Agent Skills Emerge as a New Attack Surface:** For the first time, JFrog tracked malicious AI agent skills – identifying 969 carrying high-impact payloads alongside

495 malicious AI models on Hugging Face and 56 malicious extensions on OpenVSX. Attackers are no longer just targeting code; they are targeting the autonomous tools that write, review, and deploy it.

- **Cutting through the Noise: Vulnerabilities Are Surging and Severity Scores Are Misleading:** Over 48,000 new CVEs were disclosed in 2025, a 20% year-over-year increase partially driven by AI-generated code reintroducing decades-old weaknesses, like Injection (CWE-74), which grew 3,110%. Yet the JFrog Security Research team found that 66% of CVEs analyzed had minimal real-world applicability: volume-based triage is noise, while context and applicability become the mission-critical signals.
- **The Fastest-Growing Threats Are the Least Defended:** Only 40% of organizations have adopted malicious package detection and secrets detection is active at just 28%. The categories growing fastest in threat volume remain the least covered by existing tooling.
- **Security Teams Bear the Human Cost of AI:** 45% of respondents say reviewing and hardening AI-generated code is now a major time drain – proving that AI hasn't eliminated work – it's merely shifted the burden as threat actors weaponize upstream developer environments and agentic tools.
- **The AI Governance Gap:** 97% of organizations claim they have certified model governance – yet 53% self-host models from sources where malicious payloads have been detected, and 18% have zero governance over their integrated development environments (IDE) or Model Context Protocol (MCP) servers sitting inside their developers' workflows. Thus, the gap between reported executive confidence and actual control is widening as AI development accelerates.

"The industry is operating with a false sense of security. Vulnerabilities are growing in number, but the real threat lies in threat actors hijacking our CI/CD pipelines and developer tools before code even exists," said Shachar Menashe, VP of JFrog Security Research. "Moving to automated, platform-native governance is no longer optional – it is the only way to secure the intelligent systems creating, approving, and distributing today's software."

"AI has not only changed how software is written; it has also increased the speed and scale at which zero-day vulnerabilities are exploited, and malicious software supply chain attacks are developed and distributed," said Yoav Landman, CTO and Co-Founder of JFrog. "To stay ahead, organizations need automated governance that curates every software asset entering the organization, whether introduced by agents or developers, and continuously monitors every release that contains those assets. The race is no longer about who

discovers a zero-day first, because that information is advertised within minutes. It is about who can fortify their software supply chain at scale to keep their organization secure."

To explore the full findings of this year's report and learn how your organization can close the AI governance gap, download the JFrog 2026 Software Supply Chain Security State of the Union. You can also check out our blog or register to join JFrog Security and developer experts for an upcoming webinar – *"The Illusion of Mastery: Bridging the AI Governance Gap in 2026"* **–** detailing the challenges, threats, and necessary actions for securing your software supply chain in the AI era.

###

Like this Story? Share this on X (a.k.a. Twitter): *Malicious #npm packages surged 451%; AI agent skills are now an attack surface; and 97% of orgs claim AI governance while 53% still pull models from public registries where malicious payloads have been found. The AI governance gap is real. Read the @JFrog 2026 Software Supply Chain Security report: https://bit.ly/3PRNzJB #DevSecOps #SoftwareSupplyChain #Cybersecurity #AI #governance #DevGovOps*

About JFrog
JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps, DevGovOps, and MLOps platform, is on a mission to create a world of trusted software delivery without friction from development to production. Driven by a "Liquid Software" vision, the JFrog Platform is a software supply chain system of record that is designed to power organizations as they build, manage, govern, and distribute secure software with speed and scale. Holistic security features help identify, protect, and remediate against threats and vulnerabilities. The universal, hybrid, multi-cloud JFrog Platform is available as both SaaS services across major cloud service providers and self-hosted. Millions of users and approximately 6,600 organizations worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation in the AI era. Learn more at https://jfrog.com or follow us on X @JFrog.

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

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

---

1 *JFrog commissioned 4Media Group's Atomik Research to conduct an international online survey of 1,508 IT professionals across selected industries in the United States (n=508), United Kingdom (n=125), India (n=167), Germany (n=120), France (n=125), Australia (n=165), Singapore (n=174), and Spain (n=124) between Jan-Feb. 2026. Respondents were full-time employees in IT, information systems, or technology departments holding specified job functions. All worked for organizations with 1,000+ employees and confirmed a software development team of at least 50 members. The margin of error for the overall sample is ±3 percentage points at a 95% confidence level.*