JFrog Software Supply Chain Report Shows Most Critical Vulnerabilities Scores are Misleading

74% with High or Critical CVSS scores weren't applicable in most common cases, but 60% of security and development teams still spend a quarter of their time remediating vulnerabilities

Sunnyvale, Calif. and PARIS (KubeCon + CloudNativeCon Europe), March 19, 2024 — JFrog Ltd. ("JFrog") (Nasdaq: FROG), the Liquid Software company and creators of the JFrog Software Supply Chain Platform, today released the findings of its annual Software Supply Chain State of the Union report 2024, which identifies emerging development trends, risks and best practices for securing enterprise software supply chains.

"DevSecOps teams worldwide are navigating a volatile field of software security, where innovation frequently meets demand in an age of rapid AI adoption," said Yoav Landman, CTO and Co-Founder, JFrog. "Our data provides security and development organizations with a comprehensive snapshot of the rapidly evolving software ecosystem, including notable CVE scoring errors, perspectives on the security implications of using GenAI to code, the most risky packages to allow your organization to use for development, and more, so they can make more informed decisions."

Key Findings

JFrog's Software Supply Chain State of the Union report combines JFrog Artifactory developer usage data amongst 7K+ organizations, original CVE analysis by the JFrog Security Research team, and commissioned third-party survey data of 1,200 technology professionals worldwide to provide context into the broad, rapidly evolving software supply chain landscape. Key findings include:

- **Not all CVEs are what they seem:** Traditional CVSS ratings look purely at the severity of the exploit as opposed to the likelihood it will be exploited, which requires context to make an effective assessment. The JFrog Security Research team downgraded the severity of 85% of Critical CVEs and 73% of High CVEs on average after analyzing 212 different high-profile CVEs discovered in 2023. Additionally, JFrog found that 74% of the reported common CVEs with High and Critical CVSS scores on the top 100 Docker Hub community images weren't exploitable.
- **Denial of Service (DoS) attacks reign**: Of the 212 high-profile CVEs analyzed by the JFrog Security Research team, 44% of them held the potential for a DoS attack vs. 17% with the potential to perform Remote Code Execution (RCE). This is good news for security organizations in the sense that RCE has a far more

detrimental impact vs. DoS attacks due to their ability to offer full access to backend systems.

- **Security taking a toll on productivity:** Forty percent of survey respondents said it typically takes a week or longer to get approval to use a new package/library, extending time to market for new apps and software updates. Additionally, approximately 25% of security teams' time is spent remediating vulnerabilities, even when those vulnerabilities may be overrated or even non-exploitable given their current context.
- **Applying security checks is inconsistent across the software development lifecycle (SLDC) —** The industry seems to be split pretty evenly down the middle when it comes to deciding where to apply application security testing across the software development lifecycle, underscoring the importance of shifting left and right simultaneously. Forty-two percent of developers claim it's best to perform security scans during code writing while 41% say it's best to perform scans on new software packages before bringing them into your organization from an Open-Source Software (OSS) repository.
- **Security tool sprawl continues —** Nearly half of IT professionals (47%) say they use between four and nine application security solutions. However, a third of survey respondents and security professionals (33%) say they're using 10 or more application security solutions. This supports a market-wide trend of needing security tooling consolidation with a movement away from point solutions.
- **Disproportionate use of AI/ML tools for security —** While 90% of survey respondents indicate their organization currently uses AI/ML-powered tools in some capacity to assist in security scanning and remediation efforts, only one in three professionals (32%) claim their organization uses AI/ML-powered tools to write code, indicating the majority are still wary of the potential vulnerabilities Gen-AI developed code can introduce to enterprise software.

"Vulnerabilities are growing in number year over year, but that does not necessarily mean they are growing in severity. It's clear that IT teams are willing to invest in new tools to bolster their security, but knowing where to put those tools, use their team's time, and streamline processes is critical to keeping their SDLC secure," said Shachar Menashe, Sr. Director, JFrog Security Research. "We designed this report to go beyond trend analysis, providing both counsel and clarity on the technology business leaders use to make decisions, whether it's on AI navigation, malicious code, or security solutions."

For deeper insights from the JFrog Software Supply Chain State of the Union 2024 download the full report. You can also register to join JFrog security and developer experts on Wednesday, April 17, 2024 at 10:00 a.m. PT for a webinar, *"Safeguarding Software Supply Chains in 2024: A Deep Dive into the State of the Union Report,"* detailing the challenges and complexities of managing and securing the software supply chain.

###

Like this Story? Share this: @JFrog shares research findings in their annual Software Supply Chain State of the Union 2024 report. Discover the emerging #DevSecOps trends, risks & best practices to securing enterprise #SoftwareSupplyChain. Learn more: https://jfrog.co/3TzsVNg #SoftwareSupplyChain #DevOps #DevSecOps #cybersecurity #containers #CVE

About JFrog

JFrog Ltd. (Nasdaq: FROG) is on a mission to create a world of software delivered without friction from developer to device. Driven by a "Liquid Software" vision, the JFrog Software Supply Chain Platform is a single system of record that powers organizations to build, manage, and distribute software quickly and securely, ensuring it is available, traceable, and tamper-proof. The integrated security features also help identify, protect, and remediate against threats and vulnerabilities. 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 Twitter: @jfrog.

Cautionary Note About Forward-Looking Statements

This press release contains "forward-looking" statements, as that term is defined under the U.S. federal securities laws, including but not limited to statements regarding the JFrog Software Supply Chain Report.

These forward-looking statements are based on our current assumptions, expectations and beliefs and are subject to substantial risks, uncertainties, assumptions and changes in circumstances that may cause JFrog's actual results, performance or achievements to differ materially from those expressed or implied in any forward-looking statement. There are a significant number of factors that could cause actual results, performance or achievements, to differ materially from statements made in this press release, including but not limited to risks detailed in our filings with the Securities and Exchange Commission, including in our annual report on Form 10-K for the year ended December 31, 2023, our quarterly reports on Form 10-Q, and other filings and reports that we may file from time to time with the Securities and Exchange Commission. Forward-looking statements represent our beliefs and assumptions only as of the date of this press release. We disclaim any obligation to update forward-looking statements.