JFrog Releases OSS Tools to Identify Log4j Utilization in Both Binaries & Source Code

December 16, 2021

Open-Source Tools Allow Developers to Quickly Determine Exposure & Focus Remediation Efforts to Speed Time to Resolution

SUNNYVALE, Calif.--(BUSINESS WIRE)--Dec. 16, 2021-- JFrog Ltd. ("JFrog") (NASDAQ: FROG), the Liquid Software company and creators of the JFrog DevOps Platform, today released free scanning tools specifically designed for developers to detect the presence and utilization of Apache Log4j in both source code and binaries. The four new tools are available for download immediately via GitHub in both Java and Python.

The new tools perform specialized scans to identify direct or indirect (transitive) dependencies, as well as instances where Log4j does not appear as a separate file, but is bundled inside a larger software package and harder to detect. The new tools are command line-based for easy integration with developers' existing environments and their open-core helps ensure the capabilities will continue to evolve over time as needs change.

"The Log4j vulnerability has set the enterprise software landscape on fire due to its widespread usage as a component across the software supply chain, making it difficult to rapidly pinpoint and remediate," said Asaf Karas, CTO of JFrog Security Research. "In times of crisis open-source tools that scan both binaries and source code allow community collaboration and contributions to collectively solve immediate and long-term security issues, which is why we're proud to release these tools today."

Industry research estimates nearly half of all global enterprises have already been impacted by the Log4j vulnerability with incidents rising by the day. Government officials from Austria, Canada, New Zealand, the U.K., and the U.S. have also sounded alarms over this recently exposed vulnerability and are recommending immediate action by enterprises and software providers alike.

The Log4j vulnerability was originally discovered and reported to Apache by the Alibaba cloud security team on November 24th. MITRE assigned CVE-2021-44228 to this vulnerability, which has since been dubbed Log4Shell by security researchers. JFrog's Security Research team detailed currently known Log4j vulnerabilities and outlined best practices for how to identify and address them in this blog, which is being continuously updated.

Interested parties can also register to learn more about Log4j, its impact, and how to quickly identify and manage threats in JFrog's webinar, "*Log4Shell Vulnerability: All you need to know*," taking place on Thursday, December 16, 2021 at 11 am PT/2 pm ET.

Like this Story? Tweet this: .@jfrog releases 4 new OSS tools to help identify and remediate Log4j vulnerabilities. Download them now: https://github.com/jfrog/log4j-tools

About JFrog

JFrog is on a mission to be the company powering all of the world's software updates, driven by a "Liquid Software" vision to allow the seamless, secure flow of binaries from developers to the edge. The company's end-to-end DevOps platform – the JFrog Platform - provides the tools and visibility required by modern organizations to solve today's challenges across critical pieces of the DevOps cycle. JFrog's hybrid, universal, multi-cloud DevOps platform is available as both self-managed and SaaS services on a number of cloud service provider platforms. JFrog is trusted by millions of users and thousands of customers, including a majority of the Fortune 100 companies that depend on JFrog solutions to manage their mission-critical software delivery pipelines. Learn more at jfrog.com.

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 open-source tools that allow developers to quickly determine exposure and focus remediation efforts to speed time to resolution, our ability to meet customer needs, and our ability to drive market standards. 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, 2020, 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.

View source version on businesswire.com: https://www.businesswire.com/news/home/20211216005779/en/

Press Contact:
Jfrog@bocacommunications.com

Investor Contact:
JoAnn Horne
jhorne@marketstreetpartners.com

Source: JFrog Ltd.