FACT SHEET

Kiteworks

"Log4Shell" Zero-day Vulnerability (CVE-2021-44228)

What Is Log4Shell?

"Log4Shell" or "LogJam" (CVE-2021-44228) is a critical zero-day vulnerability to the Apache Log4j Java-based, open-source logging library.[1] The Log4j library is used in enterprise software and web applications, including products from Apple, Amazon, Cloudflare, Twitter, and Steam, among many others.[2] The vulnerability was first reported to Apache by Alibaba Cloud's security team on November 24 2021.[3]

What Risk Does Log4Shell Pose?

The Log4Shell vulnerability impacts default configurations of multiple Apache frameworks, including Apache Struts2, Apache Solr, Apache Druid, and Apache Flink. Its widespread distribution poses a significant risk to both home users and enterprises alike.

Similar to past exploits like Shellshock or Heartbleed, Log4Shell is a remotely exploitable security vulnerability that can allow complete system takeover without requiring authentication. Proof-of-concept (POC) exploits are currently being distributed online and threat actors have already begun launching malware to scan for vulnerable servers.[4]

Is the Kiteworks Platform Vulnerable to Log4Shell?

We do not currently consider Log4Shell to be a P0 vulnerability in Kiteworks systems. While the recent Kiteworks 2021 Fall Release (7.6) includes the affected Apache library, our testing shows no signs of exposure to this vulnerability. Specifically, we attempted several of the publicly available POC attacks and have no indication of Log4Shell being exploited in the Kiteworks platform. Additionally, Kiteworks' multi-layered protection includes files that are individually encrypted, which means they are not exposed to this kind of vulnerability.

Is There a Kiteworks Security Patch?

Yes. As a precaution, Kiteworks released a 7.6.1 Hotfix software update to address the vulnerability. This patch release adds the mitigation for CVE-2021-44228 contained in the Solr package as recommended by Apache Solr group. Specifically, it updates the Log4j library to a non-vulnerable version on CentOS 7 systems. It also adds the recommended option "$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true" to disable the possible attack vector on both CentOS 6 and CentOS 7.

To install the 7.6.1 Hotfix update on Kiteworks:

1. Sign in to the **Admin Console** on your Kiteworks server.
2. On the toolbar, click the **System** button.
3. In the navigation pane, click **Software Update**.
4. On the Software Update page, for the Software Version Opt-In setting, click **General Availability**.
5. Near the bottom of the screen, click the **Check for Update** button. When an update is found, verify that the version number is 7.6.1 or higher.
6. Install the update, click **Download Software Update**, and then click **Run Software Update**.

We continue to proactively monitor the vulnerability to determine if any permutations occur in the threat vector that change the above assessment.

If you have any questions or issues regarding Log4Shell or the 7.6.1 patch, please contact Support: support@kiteworks.com.

[1] "National Vulnerability Database: CVE-2021-44228 Detail," NIST, December 13, 2021.

[2] Sergiu Gatlan, "New zero-day exploit for Log4j Java library is an enterprise nightmare," Bleeping Computer, December 10, 2021.

[3] "Worst Apache Log4j RCE Zero day Dropped on Internet," Cyber Kendra, December 12, 2021.

[4] Lawrence Abrams, "Hackers start pushing malware in worldwide Log4Shell attacks," Bleeping Computer, December 12, 2021.