Log4j vulnerability

Last Modified on 12/28/2022 12:24 pm EST

Recently, a vulnerability in Apache Log4j and Log4j2 has surfaced. Since we've had a few customer inquiries about this, we thought it would be best to share some more details.

Summary

Near the end of last week, a vulnerability in Apache's Log4j Java-based logging tool was identified. This vulnerability affects Log4j and Log4j2 and is being referred to as **CVE-2021-44228**.

Basically, the security issue that was found allows someone to execute arbitrary code in applications using this library, which is pretty significant.

You can read more about the vulnerability any number of places, but our security team liked the write-up in The Register: Log4j RCE: Emergency patch issued to plug critical auth-free code execution hole in widely used logging utility

The Apache Foundation has released a patch for the issue, and most vendors and software providers are working on releases to incorporate that patch or other suggested remediation steps.

Effects on KO customers

KnowledgeOwl itself does not use Java nor Apache Log4j and so is not vulnerable to CVE-2021-44228.

For due diligence, we have been reviewing all of our 3rd party vendors and software for potential risk.

We have only identified two services from one vendor in use by KnowledgeOwl that uses Log4j. The service provider has already patched one of those services; the other is in the process of being patched.

In other words, our assessment is that CVE-2021-44228 does not pose a serious risk to KnowledgeOwl or our customers. We'll be continuing to monitor as more of our vendors provide updates, and we'll let you know of any changes.

Please let us know if you have any further questions or concerns.