

thebigword



WordSynk

APACHE LOG4J / LOG4SHELL VULNERABILITIES



SUMMARY

On 2021-12-09, a vulnerability in Apache Log4j (a logging tool used in many Java-based applications) was disclosed, that could allow remote unauthenticated attackers to execute code on vulnerable systems. The vulnerability is tracked as CVE-2021-44228 and is also known as "Log4Shell".

thebigword Group is investigating to determine products (if any) that are affected and is continuously updating this advisory as more information becomes available.

PRODUCTS AND STATUS

Product Name	Status
WordSynk – Web Application All versions	Do not use the vulnerable Log4j software and have not been affected
WordSynk – Mobile Application All versions	Do not use the vulnerable Log4j software and have not been affected
WordSynk – Telephone Interpreting Application All versions	Do not use the vulnerable Log4j software and have not been affected
WordSynk Network – Web Application All versions	Do not use the vulnerable Log4j software and have not been affected
WordSynk Network – Mobile Application All versions	Do not use the vulnerable Log4j software and have not been affected
IMS.DIRECT All versions	Do not use the vulnerable Log4j software and have not been affected
IMS All versions	Do not use the vulnerable Log4j software and have not been affected
LanguageDirector All versions	Do not use the vulnerable Log4j software and have not been affected
TMS Gateway All versions	Do not use the vulnerable Log4j software and have not been affected

Internal and third-party systems All versions	We immediately took action to mitigate any potential impacts on our internal applications and systems. A full audit of our internal systems has been completed to detect unknown instances of Log4j, and if applicable, we have taken the necessary actions. That is, one identified instance of Log4j on a non-essential server has been shut down as a precautionary measure.
--	---

FINAL NOTE

We immediately took action to mitigate any potential impacts on our internal applications and systems. A full audit of our internal systems has been completed to detect unknown instances of Log4j, and if applicable, we have taken the necessary actions.

GENERAL SYSTEM SECURITY

Our WordSynk System is one of the most secure on the market. Hosted on Microsoft Azure Cloud Systems, it is one of the most secure cloud-based solutions available, with 256-bit encryption. Microsoft Azure enables additional layers of security for client's compliance through local and remote data storage.

thebigword also holds the ISO27001 for Information Security, demonstrating our commitment to providing excellent service to our clients, including excellence in how we handle their data.