Apache Log4j 2 Vulnerability (CVE-2021-44228 and CVE-2021-45046)

Summary

Inskin Media has been closely following the security vulnerabilities identified for the Log4j 2 Java logging utility and are monitoring the situation very closely. We do not currently have any open security issues but continue to monitor our own systems and the status of third parties that we work with. Given the pervasive nature of the issue we expect more product specific vulnerabilities to be uncovered continually into the future so the status of this remains open.

Background

Log4j is a commonly used utility employed by many products and services as a logging provider (e.g. to store messages in log files). The vulnerability concerns the ability to execute arbitrary code on the server where the log4j service is installed, simply by means of sending a specially formatted message through the logging system. Such messages cause a connection to be made to a remote server from where code can be pulled into the host system and executed.

By the very nature of logging systems, the servers that make use of log4j need not be connected to the public Internet to be compromised by this security issue, since logged messages may be passed into the systems through public endpoints and those messages passed onwards into protected internal systems and then logged.

System Analysis

Inskin Media do not develop in Java and therefore do not make direct use of the log4j logging system in services that we develop ourselves. This means that our primary products are not directly affected by this security issue.

We have identified the use of log4j in some internal tools and services however and have taken action to upgrade or otherwise mitigate the issues to prevent execution of remote code on our systems (or those of our partners).

The following public endpoints/services have been assessed and are not affected by the issue:

1. Ad Serving endpoints. Assessed, Unaffected
2. Reporting Systems. Assessed, Unaffected
3. Creative Studios. Assessed, Unaffected

Internal Systems

All internal systems and utilities that have so far been identified as using log4j have been upgraded according to the service providers’ latest updates (including those for the later CVE-2021-45046 vulnerability). This includes services for ElasticSearch and some internal development tools.

We are continuing to monitor the situation

Updated 2021-12-17