HISCOX
CYBERCLEAR®

Cyber Incident Report
Broker communication
14 December 2021

Recent Java Log4j exploitation: what to know and tell your clients

Reading time 2 mins

On Thursday, December 9, 2021, a Zero-day exploit was made public in the popular Java logging library Log4j. This is often used to create and store logging information from software, applications, hardware appliances etc.

Impacted versions of Log4j are 2.0 - 2.15.0, the vulnerability is fixed in version 2.16.0

How big is the risk?

This is a particularly dangerous vulnerability because the exploitation can be conducted remotely, it requires no authentication, and it can give full access to the server/device being attacked. Furthermore, it is trivial to exploit (using only a single line of code), and proof of concept attacks are already published online.

This log library is widely used, and is found in a wide range of appliances, and software from companies such as Apache Struts and Tomcat, Solr, Linux distributions, Blackberry Symantec, Apple etc.

Who's most affected?

Unfortunately, there is no specific type of organization that is likely to be affected more than another and it's difficult for an individual business to see if they're vulnerable. For example, while a customer might not have the vulnerability in their own version of the software they have written, it is entirely possible that appliances they use (such as VPN devices, cloud providers etc.) may have the vulnerability.

As this is an Apache library, it's more likely to be running on Linux servers; however, it's a Java vulnerability, and Java can run on multiple platforms. Therefore Windows, Linux and Apple servers could all be vulnerable. We suspect companies between £/$/€ 25m to 1Bn are the most at risk, due to the fact that they are likely to be running vulnerable software/devices, and they may have the skills or awareness to fix the vulnerability.

What should you tell your clients?

Key questions to ask your clients:

- Are you aware of the recent log4j vulnerability aka CVE-2021-44228 or log4shell?
- Have you assessed your exposure to it for internally developed applications?
- Have you spoken to your hardware/software/cloud vendors and assessed whether their services are impacted?
- Do you have a plan to deploy updates from outcomes of the questions above?

Apache has published a security advisory here to address this vulnerability and have released a patch to fix it (2.16.0).

Our risk engineering partner, Paladin Cyber, is available to help you and your clients navigate this issue. For an automated exploitability assessment or mitigation assistance, reach out to contact@meetpaladin.com

Further reading (please note these are external links and are not endorsed or vetted by Hiscox):

- Additional detail from Lunasec.
- List of over 180 vendors with links to their guidance (compiled by French security researcher).