SECURITY ALERT

Cyber Defense Intelligence

December 10, 2021

SECURITY ALERT: Remote Code Execution (RCE) jeopardizes any server hosting an unpatched java application.

Summary

On December 09, a Remote Code Execution (RCE) was discovered in the Java logging library log4j given CVE-2021-44228. The RCE is triggered by Java-based applications logging the exploit string and executing a remote payload that the string is pointing to. This vulnerability leaves any server hosting an unpatched java application vulnerable to exploitation. Log4j2 released version 2.15.0 on December 09, 2021, to fix the vulnerability.

Details

The vulnerability affects Log4j versions 1.0 to 2.14.1. If you are running any Java application that uses the affected log4j libraries that accept and log user input make a significant effort to patch the update. This means Java-based web applications and perhaps even network or security appliances that integrate Java as a part of their operations for enterprise customers. Java's famous tagline is that it runs on billions of devices. Apache Struts appears to be affected, but some versions of the JDK were not affected as they were secured.

Please note that log4j 2.12.1 was the last release of log4j that supported Java 7 and that patching this vulnerability may require updating the JVM to Java 8.

Mitigations

Log4j2 versions 2.10.0 and greater have a formatMsgNoLookups property which will mitigate the vulnerability if enabled. If this setting does not break anything in your application, it is recommended to enable it.

Detection

To detect exploit attempts, look for the string "${jndi:" in weblogs. If you find any results, there should also be a payload following the string. If there is allowed traffic to the payload, make sure to thoroughly investigate the server to determine what executed.

Note: Some tools have made updates to address this issue. This section will be updated as we learn of software updates.

Gytpol: Released a version which not only detects but also remediates the issue. For more details: https://gytpol.com/2021/12/13/log4j-log4shell-gytpol-not-only-discovers-but-we-can-repair-it-too/