TCPWave IPAM

Log4Shell – Zero Day Vulnerability

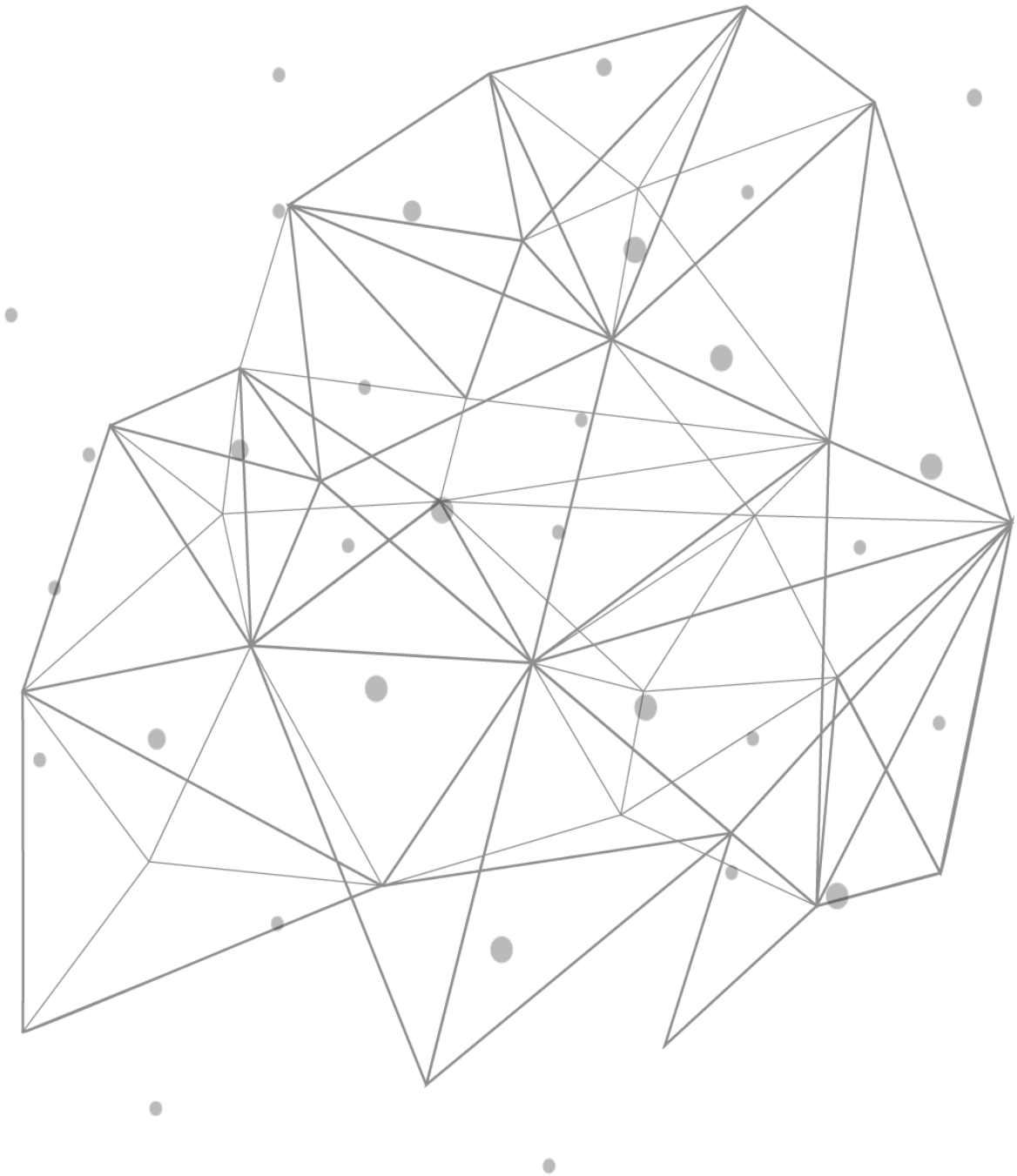


Table of Contents

Introduction

Logging is one of the fundamental features of many applications, which makes Log4j widespread. The vulnerability is called Log4Shell. Log4j is the name of the Java logging system where the exposure is found. It is an open-source software provided by the Apache Software Foundation.

Log4Shell – Zero-Day Vulnerability

The CVE-2021-44228 vulnerability was found and reported to Apache. The vulnerability allows the attacker to perform unauthenticated, remote code execution (RCE) and is triggered when a modified string provided by the attacker through various input vectors is parsed and processed by the Log4j vulnerable component.

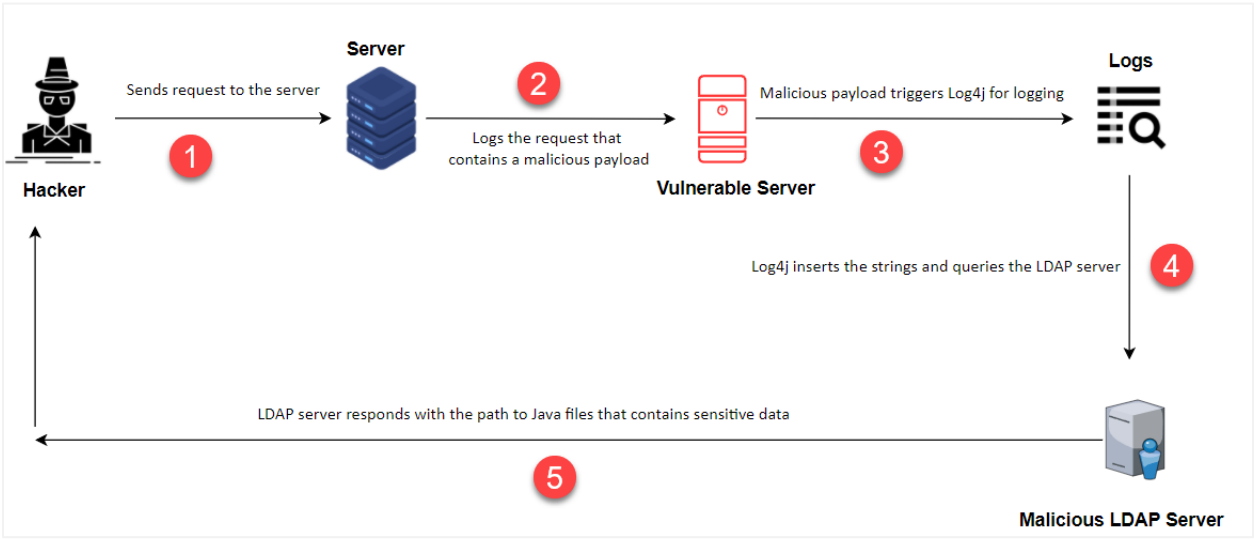
Log4j

Log4j is an extensively used and popular logging package for Java software. It records events, errors, and other system operations and communicates diagnostic messages to administrators and users.

Example: When a user clicks a web link, the system displays a 404-error message, then the webserver running the domain informs the user that there is no such webpage. Log4j records this particular event in a log for the server's system administrators using Log4j to perform specific diagnoses.

Flow

The following diagram explains how the vulnerability works:



TCPWave Recommendation

As the Log4j vulnerability requires defense-in-depth, TCPWave recommends that enterprises deploy rules to block the exploiting traffic. Besides that, an enterprise that uses the log4j library needs to upgrade to log4j 2.17.1 version immediately.

Conclusion

TCPWave's DDI solution helps our customers manage and modernize their enterprise-grade solutions by ensuring they have the most innovative technology with minimal risks.

For a quick demo, contact the TCPWave Sales Team.