White Paper

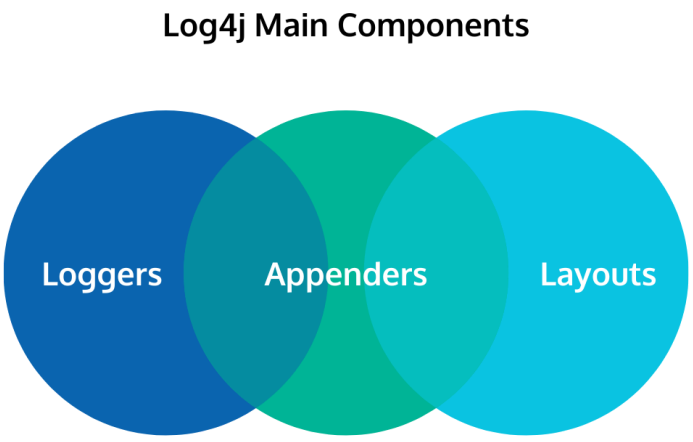
Log4j Vulnerability - Managing Enterprise Security

Everything you need to know about vulnerability Log 4j that can have serious consequences for enterprise software systems. Log4j enables attackers to run arbitrary code remotely on targeted systems/servers.

TABLE OF CONTENTS

INTRODUCTION

Logging has become a non-evitable part of every web application and server-based program. These special file types keep logs (i.e., records) of events or actions happening within the application. Log4j is a universally employed software logging library for Java software. On 9 December 2021, information was publicly announced as the critical security vulnerability in the library by Apache Foundation. This is called the Log4j (Log4Shell) vulnerability. It impacted Minecraft servers. A week later, researchers found that millions of devices are at risk due to this vulnerability.



The following observations make the tacking of this vulnerability a priority for all enterprises and software vendors:

1. As Log4j allows remote code execution, hackers can compromise a system entirely.
2. The Log4j library is hugely employed by many software for logging events, making various organizations vulnerable.

3. Since logging is used in different applications and circumstances, attacks are invited in various ways.
4. It is effortless to attack; just a simple string/thread in a request or a message is needed to be logged to introduce attacks. And, it works every time, even without the user's consent to click on the link or misconfigure/interrupt the entire system.

This white paper will discuss the most-talked vulnerability in the current technological landscape and the steps to mitigate the risk for enterprise software systems.

ABOUT LOG4J AND HOW IT IS USED

An authentic procedure for debugging software incorporates log statements inserted into the code during the software development lifecycle. Log4j, which is both reliable and feasible, is among such logging libraries for Java.

It is developed and maintained by Apache Software, an open-source foundation; Log4j can operate on Windows, Linux, and Apple's macOS.

In order to probe the state of the system during runtime, logging is an essential approach in software development. Availability of system activity logs can be helpful to monitor the system at any stage/phase of development. Therefore, developers employ Log4j across different phases of development alongside online gaming, cloud-based data centers, and enterprise software.

Collectively Log4j has three major components-loggers, appenders, and layouts. All work combined to make logging in a systematic manner effective.

WHAT IS LOG4J VULNERABILITY?

The Log4j vulnerability allows threat actors to have a stronghold across web-facing servers by introducing malicious text strings. It exists inside the Log4j, a library for logging errors and events in Java-based

applications.

Log4j serves as a third-party logging solution for software professionals to log data inside an application without fabricating any customized solution.

Put simply, hackers can steal confidential information or take advantage of available resources. This vulnerability can reveal organizations to new heaps of cybersecurity risks where attackers can exploit remotely.

Moreover, attackers can control log messages and log message parameters and manipulate different versions of Log4j to commend arbitrary codes and attain complete control of the targeted servers.

It has been widely reported that hackers are taking advantage of this vulnerability to deploy crypto miners and other potential worms, viruses, and spyware. This vulnerability provides hackers a path to install ransomware inside the system. Ransomware is a type of computer virus sealing up data and systems until victims pay them to unlock the system.

WHERE DID LOG4J GET DETECTED FOR THE FIRST TIME?

According to CBS News, a group of people from the Apache Software Foundation group got the alert on November 24 about the vulnerability. A cloud security team member of Alibaba discovered it for the first time. It came to the limelight when cybersecurity professionals shared a blog post about Minecraft leveraging this vulnerability in the first week of December. That blog alerted the gamers about the cybercrime detected through that flaw and infiltrations into their computers.

WHAT TYPES OF SOFTWARE SYSTEMS ARE AT RISK?

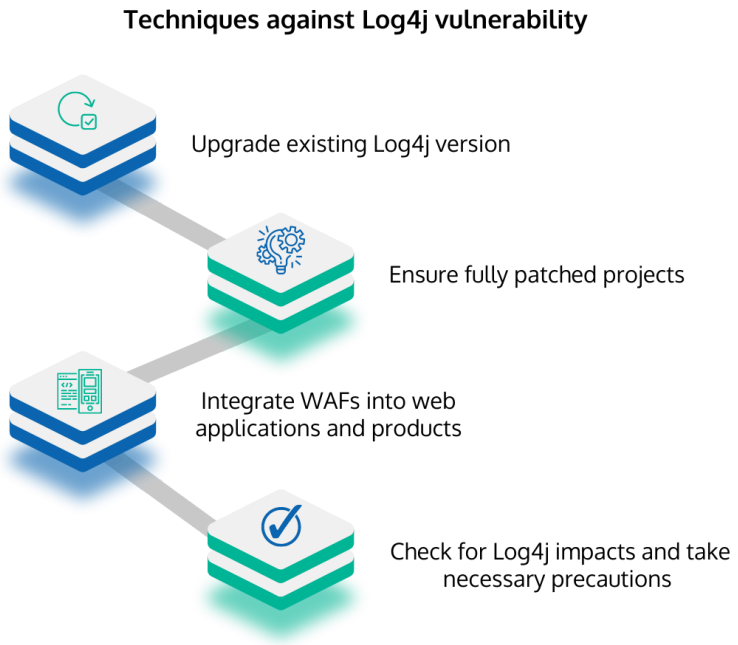
Around the globe, all the Java-based companies and servers hugely deploy the Log4j library. Due to global utilization across applications and digital services, many products are vulnerable to exploitation. Additionally, it may harm any device running over Apache Log4j version 2.0 to

2.14.1 via accessing the internet. To name a few, Apple's iCloud, Microsoft's Minecraft, LinkedIn, Twitter, Amazon, Google, etc, use Apache Log4j.

Being recognized as the zero-day vulnerability, Log4j is subjected to many backlashes. If a program is not provided with a latch, it encourages attackers to crash the system, steal sensitive information, and contaminate networks with malicious software/activities.

HOW TO PREVENT AN LOG4J ATTACK

Enterprises should do the following actions whether an attack is experienced or not. Start by searching the application logs to check if any RCE payload resides or not. If keywords like "ldap", "jndi", "$ {::" come during the search, you should further investigate as to whether it's a fingerprinting by security professionals or an actual attack. Here is a checklist of some standard prevention techniques you can use against Log4j vulnerability.



- Enterprises should upgrade their existing Log4j version to Log4j version 2.16.0. It got officially released on December 13 by Apache. According to Apache, if any project is still leveraging the old version of Java, i.e., Java 7, they should immediately upgrade to Log4j 2.12.2.

- Ensure that all your project or product dependencies, APIs, and libraries are fully patched.

- Some well-known Web Application Firewall (WAF) vendors announced that their WAF could protect against the Log4j vulnerability. So, another good practice is to integrate these WAFs into your web applications and products.

- If a software vendor developed or provided your application, it is always good to consult them to verify whether they got impacted by log4j. If so, ask them if they have come up with a patch for the products.

CONCLUSION

Log4j is a critical vulnerability, and enterprises should not ignore its impact on the overall security and data breaching abilities. Cybercriminals are still leveraging its benefits and exploiting applications that are still using the unpatched version of Log4j. However, if you believe that past behavior indicates future performance, then probably the Log4j vulnerability will crop up in the coming years.

At Batoi, we have run generalized scans in our servers, including a Clamscan antivirus scan and a general search for jar/war files; these did not throw up any result. The only cPanel component known to be vulnerable now, 'cpanel-dovecot-solr', is not installed on any of our servers.

ABOUT BATOI

Software Development Automation Company.

Batoi is a software development automation company. Batoi Rapid Application Development (RAD) Platform provides tools for designing and building applications, handling codebase deployment and security, integrating blockchain, AI, AR/VR, and IoT capabilities, and managing software projects. Batoi has been catering to customers across the globe for building, deploying, and managing their software applications since 2010.

batoi.com/research/publications