Log4j And Its vulnerlabilities

What is Log4j?

- According to wikipedia : Apache Log4j is a Java-based logging utility originally written by Ceki Gülcü. It is part of the Apache Logging Services, a project of the Apache Software Foundation. Log4j is one of several Java logging frameworks.

- Developer(s) Apache Software Foundation
- Initial release January 8, 2001; 20 years ago
- Stable release 2.16.0 / December 13, 2021;
- Repository github.com/apache/logging-log4j2
- Written in Java
- Operating system Cross-platform
- TypeLogging
- License Apache License 2.0
- Website logging.apache.org/log4j/2.x/

Log4Shell vulnerability

- A zero-day vulnerability involving remote code execution in Log4j 2, given the descriptor "Log4Shell" (CVE-2021-44228), was found and reported to Apache by Alibaba on November 24, 2021, and published in a tweet on December 9, 2021. Affected services include Cloudflare, iCloud, Minecraft: Java Edition, Steam, Tencent QQ, and Twitter.The Apache Software Foundation assigned the maximum CVSS(Common Vulnerability Scoring System) severity rating of 10(critical) to Log4Shell, as millions of servers could be potentially vulnerable to the exploit.The vulnerability was characterized by cybersecurity firm Tenable as the "the single biggest, most critical vulnerability of the last decade" and Lunasec's Free Wortley characterized it as "a design failure of catastrophic proportions".
- This vulnerability allows attackers to execute code remotely on a target computer, meaning that they can steal data, install malware or take control.
- The feature causing the vulnerability could be disabled with a configuration setting, which had been removed in Log4j version 2.15.0-rc1 (officially released on December 6, 2021, three days before the vulnerability was published), and replaced by various settings restricting remote lookups, thereby mitigating the vulnerability.For additional security, all features using JNDI(Java Naming and Directory Interface API), on which this vulnerability was based, will be disabled by default, and support for message lookups removed from version 2.16.0 onward.

Thank you!!