Log4Shell Vulnerability

For Prelims: Log4Shell, open-source logging software Apache Log4J, vulnerability in computer security, Application Logging

For Mains: Impact of Log4Shell Vulnerability on India and World.

Why in News

A critical vulnerability called **Log4Shell**, detected last week in widely used **open-source logging software Apache Log4J**, is now being exploited by attackers to target organizations all over the world, including India.

- The vulnerability is **based on an open-source logging library** used in most applications by enterprises and even government agencies.

Vulnerability

- In computer security, a **vulnerability is a weakness which can be exploited** by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system.
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. The vulnerabilities are **also known as the attack surface.**

Application Logging

- Application Logging is the process of **saving application events.** It varies from other event logs within IT systems in that the information collected by an application event log is dictated by each individual application, instead of the operating system.
- They help **provide visibility into how our applications are running** on each of the various infrastructure components.
- **Log data** contains information such as out of memory exceptions or hard disk errors.

Key Points

- **Name:**
  - The vulnerability is dubbed **Log4Shell** and is officially called **CVE-2021-44228.**
  - CVE number is the unique number given to each vulnerability discovered across the world.
  - The vulnerability was first detected on websites that were hosting servers of a Microsoft-owned game called **Minecraft.**
- **Log4j library:**
  - Log4j is open-source software maintained by a group of **volunteer programmers** as part

of the nonprofit **Apache Software Foundation** and is a key **Java-logging framework.**
    - The **Log4j library** is embedded in every **Java-based web service** or **application** and is used by a wide number of companies to enable **logging in on applications.**
        - **Java** is one of the most commonly used programming languages in the world.
    - The **problem impacts Log4j 2 versions** which is a very **common logging library** used by applications across the world.
        - Logging lets developers see all the activity of an application.
    - Tech companies such as Apple, Microsoft, Google all rely on this open-source library, as do enterprise applications from CISCO, Netapp, CloudFare, Amazon and others.
- **Severe Rating:**
    - Log4Shell has been assigned a **severity rating of 10** by security experts, the highest level possible.
    - The vulnerability could allow a hacker to take control of a system.
        - Data supplied by an untrusted outsider – data that you are merely printing out for later reference, or logging into a file – **can take over the server on which you are doing the logging.**
        - This **could turn** what should be a basic **"print" instruction into a leak-some-secret-data-out-onto-the-internet situation**, or even into a download-and-run-my-malware-at-once command.
        - Simply put, a log entry that you intended to make for completeness, perhaps even for legal or security reasons, **could turn into a** malware **implantation event.**
- **Remote Code Execution:**
    - The vulnerability can be **exploited by using a single line of code** and **allows attackers to execute remote commands** on a victim's system.
    - It can be exploited by attackers to take control of any Java-based web server and carry out **Remote Code Execution (RCE) attacks.**
    - In an RCE attack, attackers take control over the targeted system and can perform any function they want.
    - The exploits for this vulnerability are already being tested by hackers, according to several reports, and it grants them access to an application, and could potentially let them run malicious software on a device or servers.
- **Impact of Log4Shell Vulnerability:**
    - **Cryptocurrency Mining:** Most of the attacks they have observed appear to **focus on the use of** cryptocurrency **mining** at the expense of the victims. However, new variations of the original exploit are being introduced rapidly.
        - Successful exploitation of this vulnerability could **lead to disclosure of sensitive information,** addition or modification of data, or **Denial of Service (DoS).**
    - **Global:** The **Australia-New Zealand (ANZ) area** was the most impacted region with **46% of corporate networks facing an attempted exploit.**
        - While North America was the least impacted with 36.4% of organizations facing such an attempt.
    - **India**: About 41% of corporate networks in India have already faced an attempted exploit.
        - Indian companies are not more vulnerable than their western counterparts because **they use Java-based applications.**
        - **Indian companies are at high risk** because of their weak security posture, especially the smaller companies that may not have the know-how or resources to detect and fix the issue quickly.

Source: IE