Log4 Shell

December 15, 2021

In news– Recently, the Log4j vulnerability also known as Log4 Shell has been reported and affected a wide range of products including Amazon, Twitter and Apple's iCloud.

About Log4 Shell-

- This software flaw as reported by cybersecurity researchers could **allow attackers to have uncontrolled access to computer systems.**
- It was **first highlighted by researchers at LunaSec.**
- The issue was **discovered in Microsoft-owned Minecraft, though LunaSec warns that "many, many services" are vulnerable to this exploit due to Log4j's "ubiquitous" presence.**
- It **can allow an attacker to control and execute 'arbitrary code'** and **gain access to a computer system.**
- It can allow a hacker to gain complete **control of a server** when exploited correctly.
- The Log4j library in Java is used to keep a record of all activity in an application and is thus very commonly used by software developers across the world.
- It supports by default a logging feature called "Message Lookup Substitution".
- This feature enables certain special strings to be replaced, at the time of logging, by other dynamically-generated strings.
- It is **dubbed as CVE-2021-44228** which is the official name given to each software vulnerability as it is discovered.
- The technical definition in the CVE library states that "An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled."
- The worrisome part here is that the exploit has likely been used by hackers to gain access to certain computer

systems, and now that the exploit is in the open, companies will have to patch it soon.