Log4Shell zero-day vulnerability discovered, the new nightmare of enterprises

How to exploit a critical zero-day vulnerability in the Java-based Apache Log4j logging library has just been posted on the internet. This leaves users and businesses as well as organizations vulnerable to remote code execution attacks.

Log4j is developed by the Apache Foundation and is widely used by both enterprise applications and cloud computing services.

As a result, anything from enterprise software to web applications and products from Apple, Amazon, Cloudflare, Twitter, and Steam can be vulnerable to remote code execution (RCE) attacks. Even users are at risk because some popular games like Minecraft still use Java.

Hackers are actively looking for victims

The new zero-day vulnerability is tracked under the code CVE-2021-44228 and is named Log4Shell or LogJam. Successfully exploiting this vulnerability, hackers can take control of all systems with Log4j installed from version 2.0-beta9 to version 2.14.1.

Alibaba Cloud's security team reported this vulnerability to Apache on 11/24. They also revealed that CVE-2021-44228 affects default configurations of many Apache frameworks including Apache Strust2, Apache Solr, Apache Druid, Apaceh Flink, etc.

After the first Log4Shell exploit was shared on the Internet on December 9, hackers actively scoured the internet for vulnerable systems. They target systems that contain vulnerabilities but are not heavily protected, do not

require authentication, and can be exploited remotely.

Patches and damage reduction methods are available

Apache has now released Log4j version 2.15.0 to address the critical vulnerability CVE-2021-44228.

Vulnerabilities can also be reduced if you set the "log4j2.formatMsgNoLookups" system property to "true" or remove the JndiLookup class from the classpath. This damage reduction method only works with Log4j version 2.10 and above.

Researchers from cybersecurity company Cybereason have also released a "vaccine" package called Logout4Shell that can be installed onto a vulnerable Log4j server remotely to reduce the vulnerability of the vulnerability.

You can learn more about Logout4Shell by visiting the link here.

Minecraft is currently actively looking for ways to patch CVE-2021-44228 while a series of agencies and organizations have warned about this vulnerability.