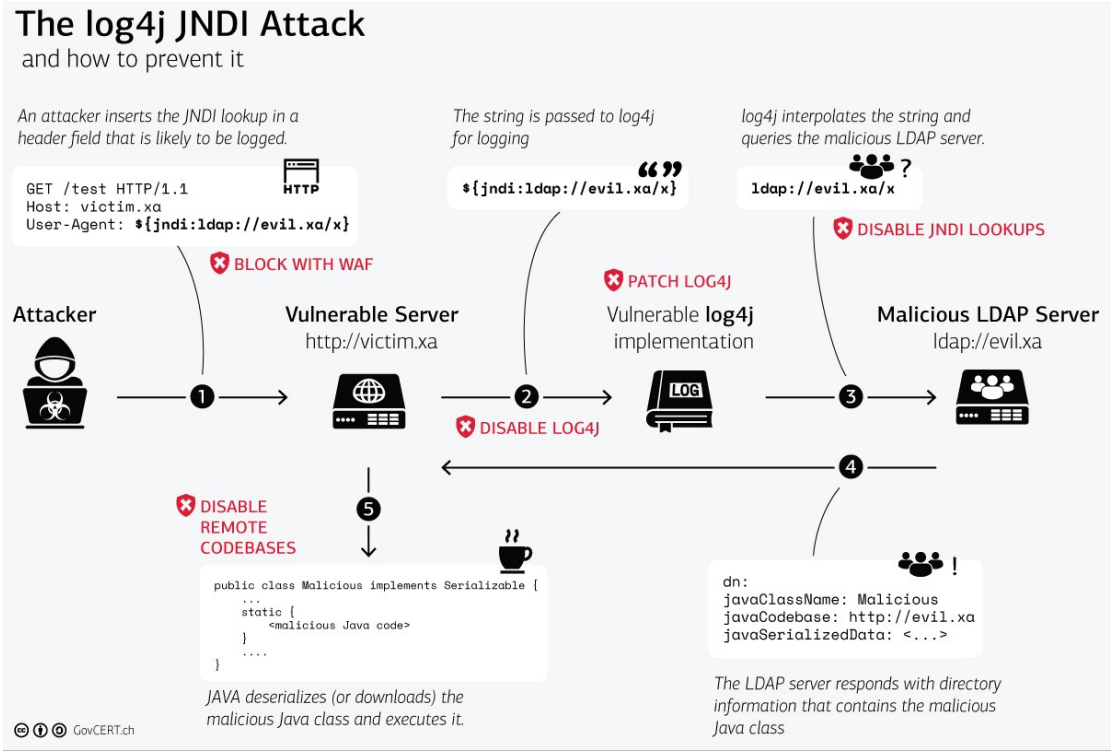
LOG4SHELL: RCE 0-DAY EXPLOIT FOUND IN LOG4J 2, A POPULAR JAVA LOGGING PACKAGE

On Thursday (December 9th), a 0-day exploit in the popular Java logging library log4j (version 2) was discovered that results in Remote Code Execution (RCE) by logging a certain string. Given how ubiquitous this library is, the impact of the exploit (full server control), and how easy it is to exploit, the impact of this vulnerability is quite severe. A new critical 0-day vulnerability impacting multiple versions of the popular Apache Log4j 2 logging library was publicly disclosed that, if exploited, could result in Remote Code Execution (RCE) by logging a certain string on affected installations.



Reference Document: https://govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

1. HOW TO INDENTIFY VULNERABLE REMOTE SERVERS

The simplest way to detect if a remote endpoint is vulnerable is to trigger a DNS query. The exploit will cause the vulnerable server to attempt to fetch some remote code. By using the address of a free online DNS logging tool in the exploit string, we can detect when the vulnerability is triggered.

In analysing CVE-2021-44228, NET SQUARE has determined the following:

- Default installations of widely used enterprise software are vulnerable
- The vulnerability can be exploited reliably and without authentication
- The vulnerability affects multiple versions of Log4j 2

- The vulnerability allows for remote code execution as the user running the application that utilizes the library
- Upgrading the underlying version of Java alone is insufficient to prevent exploitation of the vulnerability.

2. CALL TO ACTION

- **Conduct an extensive infrastructure and software/web application audit** to identify all systems that implement the Apache Log4j2 logging framework. Then, either immediately upgrade these deployments to Log4j version 2.16.0 (Updated recommendation December 14th 2021 as 2.15 has now been reported by Apache as susceptible to a Denial of Service attack) and deploy the configuration mitigations recommended by Apache.
- **Seek mitigation countermeasures or patches for all affected systems** This is especially true for software/ web applications you are running on internet-facing systems but should not be limited to such systems due to the lateral attack threat posed by the severity of this vulnerability.
  Upgrading to the patched versions of Log4j 2 or impacted applications will eliminate this vulnerability. We recommend any organization that believes they may be impacted to update to a patched version urgently.
- **Implement defence in depth approach**. As of now, attacks consist of multiple stages, giving security team a good opportunity to prevent security incident from evolving into a security breach. We have seen various modules preventing the exploitation, from network level protection (URL/IP reputation), static antimalware (detecting miner or known malicious payload) to Advanced Threat Défense for detecting suspicious process behaviour.
- Actively monitor the infrastructure for potential exploitation attempts and respond accordingly. Implement endpoint threat detection and response (ETDR) solutions, look for any signs of reverse TCP shells, and review any detected anomalies.
- Net Square encourages all organizations to adopt an assumed breach mentality and review logs for impacted applications for unusual activity.
- If you find these hashes in your software inventory then you have the vulnerable log4j library in your systems and need to take action: https://github.com/mubix/CVE-2021-44228-Log4Shell-Hashes
- If anomalies are found, we encourage you to assume this is an active incident, that you have been compromised and respond accordingly.

This is an evolving situation, if you need help – please reach out to us at info@net-square.com. We are committed to helping the our clients not only understand but respond quickly to this situation.