Apache Log4j Vulnerability – Why It's Dangerous and How to Prevent a Breach

Late last week, Apache announced a flaw in its Log4j utility, a widely used Java logging library. Apache quickly released a patch for the Log4j vulnerability, but cybersecurity experts have already detected millions of exploit attempts. And they warn that the problems have just begun.

Why is the Log4j Vulnerability So Dangerous?

The Log4j vulnerability presents a significant danger for several reasons. In the first place, developers around the world use Java. Consequently, the flaw affects millions of applications and services, thus putting millions of organizations at risk. Essentially, any application or service that connects to the internet represents a potential attack point.

Second, bad actors can easily exploit the Log4j flaw, even with minimal programming skills. And they do not need to authenticate to gain access. Once in the targeted system, they can take control of servers or move laterally through an organization's network. This allows attackers to steal data, install malware or conduct cryptomining operations.

Third, finding instances of unpatched Log4j poses the proverbial needle in a haystack problem. The utility has been downloaded 84 million times in the past four months alone. And for as long as the flaw remains unpatched in an application, bad actors can walk right in.

Finally, while no breaches have been reported in the first week of the crisis, security experts have reported troubling signs. It appears that "initial access brokers" are using the vulnerability to gain access to target systems with the intent to sell that access. That is, they enter the system and create a backdoor. Then they sell that access to sophisticated cybercriminals.

In fact, Microsoft reported that state-sponsored groups from Iran, China, Turkey, and North Korea have begun exploiting the flaw. Soon, these groups are likely to use the access to initiate ransomware and other malicious attacks. In fact, Bitdefender reported evidence of hackers already trying to deploy the Khonsari ransomware.

Apply Patches Quickly

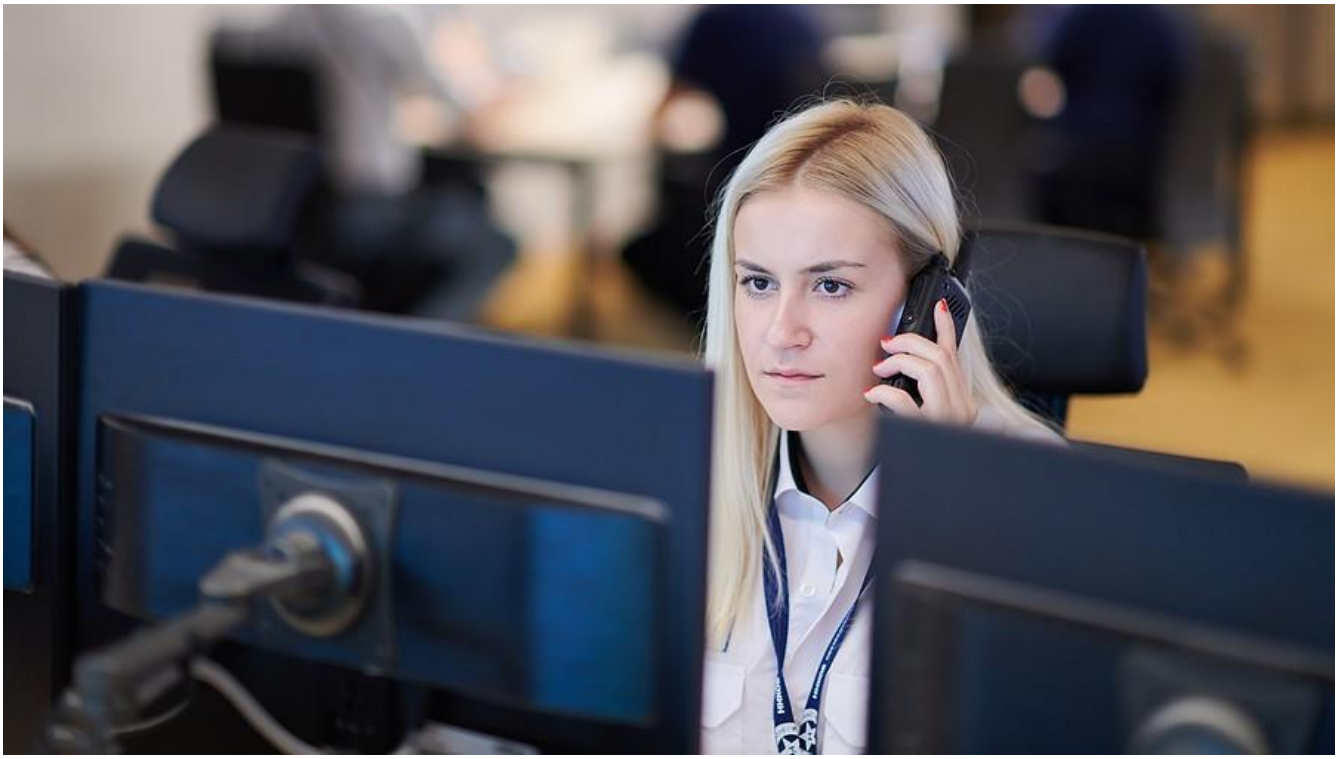
The first step in mitigating the Log4j vulnerability involves patching. Apache released an initial security patch for Log4j on December 10 (version 2.15.0). When they discovered a second vulnerability days later, they released a second patch (version 2.16.0). Developers must upgrade to 2.16.0 as soon as possible.

Organizations and individuals should keep an eye out for notices from their software vendors. Once vendors patch their own systems, they will release security updates of their products, which organizations should apply quickly.

Address the Supply Chain

Like the SolarWinds hack last year, the Log4j vulnerability highlights supply chain issues. Even if a vendor does not directly use Log4j, for instance, they likely use a widget or an open-source library that utilizes Log4j. In fact, a single product may use dozens of parts developed by third parties.

Consequently, organizations need to check in with the vendors in their supply chain. Ask if they use Log4j. If they do, learn if they have provided security patches for the products you use.



Monitor for Suspicious Activity

While security experts have made it clear that patching is critical, patches alone will not guarantee safety from hackers exploiting the Log4j vulnerability. Because of the lag between appearance of the flaw and patching, hackers may have already taken up residence. And they can prove very difficult to detect.

Organizations should take a conservative approach and constantly monitor their networks for any suspicious behavior. A reputable security provider will offer monitoring tools that provide 24/7 threat detection to proactively detect potential problems.

Implement Cybersecurity Best Practices

As the past few years have shown, cyber threats continue to evolve at a rapid pace. The Log4j vulnerability follows a long line of threats, from WannaCry to Kaseya to SolarWinds. And other threats will follow the Log4j exploits. No quick fix will keep organizations safe.

However, investing in cybersecurity and consistently following information security best practices will help organizations protect critical data assets. These best practices include firewalls and antivirus tools, regular security audits, cybersecurity training for employees, endpoint security, encryption and more.

The cybersecurity experts at eMazzanti will help you assess your current security position and design a comprehensive strategy to keep your business safe moving forward.