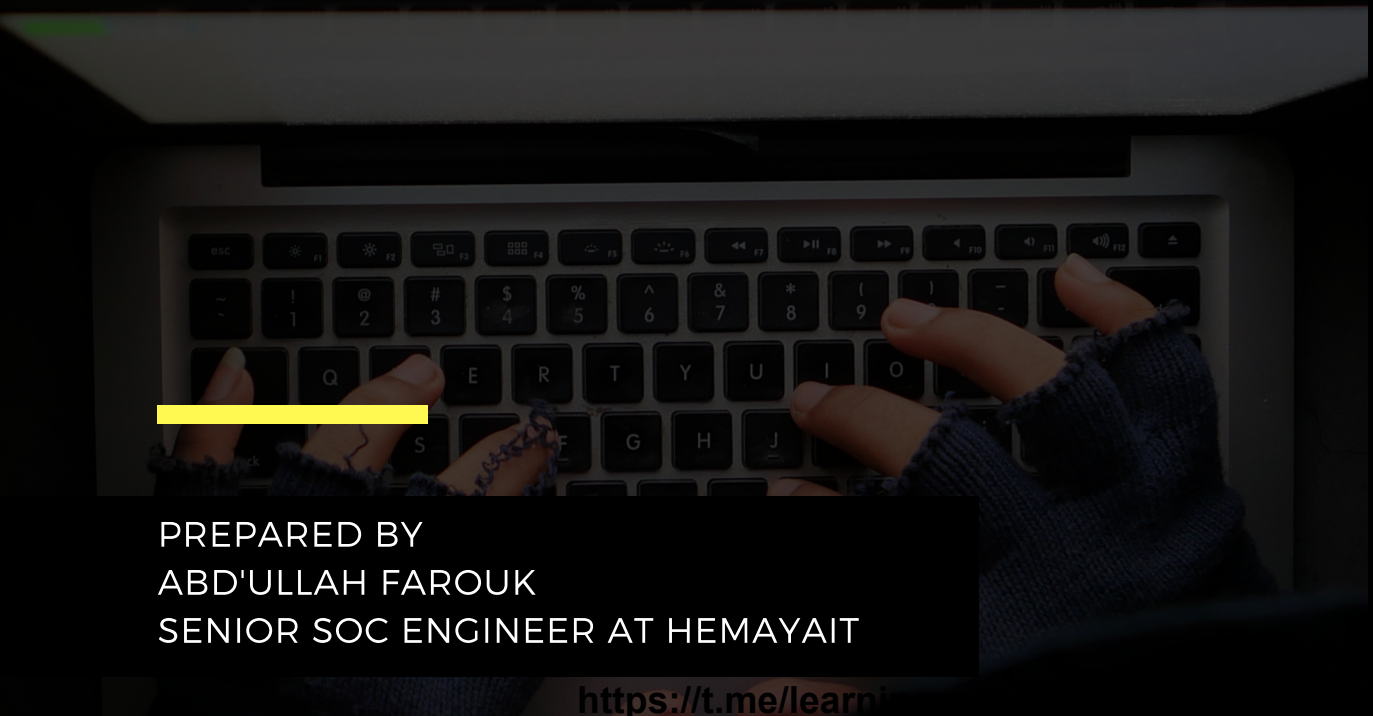
CVE-2021-44228

LOG4SHELL REPORT

VULNERABILITY ASSESSMENT AND MITIGATION



PREPARED BY
ABD'ULLAH FAROUK
SENIOR SOC ENGINEER AT HEMAYAIT

LOG4SHELL

Summary

LOG4SHell, **Zero-day** exploit in the popular Java logging library **log4j2** was discovered that results in **Remote Code Execution (RCE)** by logging a certain string.

Log4j2 is an open-source, Java-based logging framework commonly incorporated into Apache web servers and Spring-Boot web applications.

The vulnerability has been reported with **CVE-2021-44228** against the log4j-core jar. CVE-2021-44228 is considered a critical flaw, and it has a base CVSS score of 10, **the highest possible severity rating.**

Who is Impacted !!

Too many services are vulnerable to this exploit as log4j is a wild rang used Java-based logging utility. Cloud services like Steam, Apple iCloud, and applications like Minecraft have already been found to be vulnerable.

Anybody using Apache frameworks services or any Spring-Boot Java-based framework applications uses log4j2 is likely to be vulnerable.

APACHE HTTP SERVER PROJECT

Java EE™

spring

LOG4SHELL

HOW THE EXPLOIT WORKS !!

The exploit works when there is a service or application running with vulnerable version of **log4j2**.

Attacker who can control log messages or log message parameters can execute arbitrary code on the vulnerable server loaded from LDAP servers **when message lookup substitution is enabled.**

Info you have to know about LOG4SHELL exploit !

- Affected Apache log4j2 Versions
- Exploit Requirements
- Exploit Steps

Affected Apache log4j2 Versions

2.0 <= Apache log4j <= 2.14.1

Exploit Requirements

- A server with a vulnerable log4j version.
- An endpoint with any protocol (HTTP, TCP, etc) that allows an attacker to send the exploit string.
- log statement that logs out the string from that request.

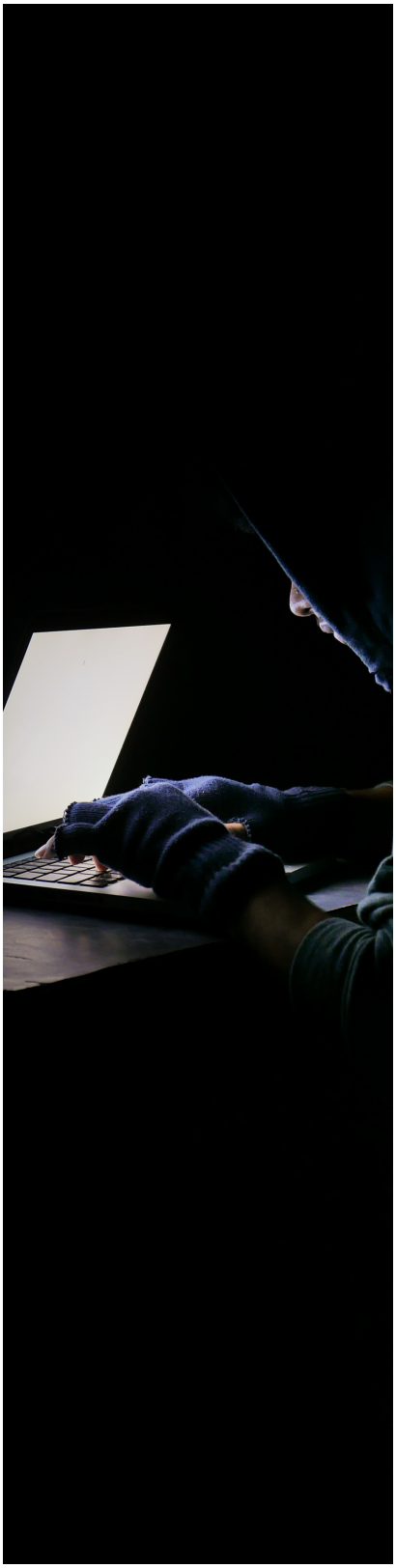
Exploit Steps

- Data from the User gets sent to the server (via any protocol),
- The server logs the data in the request, containing the malicious payload.
- The log4j vulnerability is triggered by this payload and the server makes a request to attacker.com via (JNDI),
- This response contains a path to a remote Java class file which is injected into the server process,
- This injected payload triggers a second stage, and allows an attacker to execute arbitrary code.

Arbitrary Code, In computer security, arbitrary code execution (ACE) is an attacker's ability to run any commands or code of the attacker's choice on a target machine or in a target process

LOG4SHELL

HOW TO MITIGATE



SPOT VULNERABLE APPLICATIONS

"Ask admin/system team to run a search/grep command on all servers to spot any file with name "log4j2", Then check if it is a vulnerable version or not"

PERMANENT MITIGATION

"Version 2.15.0 of log4j has been released without the vulnerability. log4j-core.jar is available on Apache Log4j page below, You can download it and updated on you system "

(https://logging.apache.org/log4j/2.x/download.html)

TEMPORARY MITIGATION

"Add "log4j.format.msg.nolookups=true" to the global configuration of your server/web applications"

LOG4SHELL

VENDOR PROTECTION

"Vendors rules and filters provide LIMITED protection against the behavior around the exploit, but it is NOT a full replacement for the actual "LOG4J" vendor patch. We should not be setting any expectation that these protections are good enough on their own to completely protect against any exploits"

LOG4SHELL

REFRANCES

- https://www.lunasec.io/docs/blog/log4j-zero-day/#how-the-exploit-works
- https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/
- https://www.techtarget.com/searchsecurity/news/252510818/Critical-Apache-Log4j-2-bug-under-attack-mitigate-now
- https://spring.io/blog/2021/12/10/log4j2-vulnerability-and-spring-boot
- https://success.trendmicro.com/solution/000289940
- https://www.contrastsecurity.com/security-influencers/0-day-detection-of-log4j2-vulnerability
- https://github.com/Puliczek/CVE-2021-44228-PoC-log4j-bypass-words
- https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/
- https://www.sentinelone.com/blog/cve-2021-44228-staying-secure-apache-log4j-vulnerability/
- https://kc.mcafee.com/corporate/index?page=content&id=KB95091
- https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce