**Subject:** Urgent: Action Required for Apache Log4j Vulnerability (CVE-2021-44228)

**To:** Infrastructure Team

**CC:** Security Operations Center (SOC), IT Leadership

Dear Infrastructure Team,

This is to alert you to a critical zero-day vulnerability in Apache Log4j (CVE-2021-44228), also known as Log4Shell. This vulnerability has been classified as **Critical (CVSS 10.0)** and poses a significant risk to our infrastructure.

**Risk/Impact**

The Log4j vulnerability allows for **remote code execution (RCE)**. Attackers can exploit this by crafting a specially formatted string that forces the vulnerable server to fetch and execute arbitrary code from a malicious server.

**Potential impact includes:**

* Full system compromise.
* Data exfiltration and loss of sensitive information.
* The ability for attackers to pivot within the network.

**Method of Exploitation**

1. The attacker sends a malicious payload leveraging Java Naming and Directory Interface (JNDI) lookups, typically embedded within user-controlled input (e.g., headers, form inputs, or log messages).
2. The vulnerable server processes the payload, making an outbound connection to a malicious server.
3. The attacker’s server responds with a payload, enabling arbitrary code execution.

This exploit requires no authentication and is being actively used in the wild.

**Remediation Steps**

1. **Immediate Patch:**
   * Update Log4j to version **2.17.0** or the latest available patched version.
   * For systems where patching is not immediately possible, implement mitigations below.
2. **Mitigations:**
   * Set the system property log4j2.formatMsgNoLookups to true:

-Dlog4j2.formatMsgNoLookups=true

* + Remove the JndiLookup class from the classpath by running:

zip -q -d log4j-core-\*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

1. **Detection and Monitoring:**
   * Check logs for suspicious JNDI lookups (ldap://, rmi://, etc.).
   * Block outbound traffic to untrusted domains at the firewall.
2. **System Audit:**
   * Identify all applications and services using Log4j.
   * Assess exposure of these systems and ensure proper patching or mitigations.
3. **Communication and Documentation:**
   * Inform all relevant teams and maintain a clear incident response plan.
   * Document remediation actions and verify their effectiveness.

For further assistance or clarification, please contact the Security Operations Center immediately at [SOC contact details].

Thank you for addressing this critical vulnerability promptly.

Best regards,  
AIG Cyber & Information Security Team