From: AIG Cyber & Information Security Team  
To: product@email.com  
Subject: Security Advisory concerning Product Development Staging Environment  Log4j  
—  
Body:  
Hello John Doe,

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

Vulnerability description

[Log4Shell](https://nvd.nist.gov/vuln/detail/CVE-2021-44228), disclosed on December 10, 2021, is a remote code execution (RCE) vulnerability affecting Apache’s Log4j library, versions 2.0-beta9 to 2.14.1. The vulnerability exists in the action the Java Naming and Directory Interface (JNDI) takes to resolve variables. Affected versions of Log4j contain JNDI features—such as message lookup substitution—that do not protect against adversary-controlled Lightweight Directory Access Protocol (LDAP), Domain Name System (DNS), and other JNDI-related endpoints.

An adversary can exploit Log4Shell by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows the adversary to take full control over the system. The adversary can then steal information, launch ransomware, or conduct other malicious activity.

Vulnerability risk/impact  
Log4Shell and CVE-2021-45046—rated as critical vulnerabilities by Apache—are severe because Java is used extensively across IT and OT platforms, they are easy to exploit, and applying mitigations is resource intensive. Log4Shell is especially critical because it allows malicious actors to remotely run code on vulnerable networks and take full control of systems.

Vulnerability remediation

1. Identify vulnerable assets in your environment.

A. Inventory all assets that make use of the Log4j Java library.

B. Identify the inventoried assets that are likely vulnerable.

2. Mitigate known and suspected vulnerable assets in your environment.

A. Treat known and suspected vulnerable assets as compromised.

B. Patch Log4j and other affected products to the latest version.

C. Keep an inventory of known and suspected vulnerable assets and what is done with them  throughout  this process.

D. Verify the mitigation has worked, if possible.

3. Initiate hunt and incident response procedures.

A. Hunt for signs of exploitation and compromise.

B. If compromise is detected, organizations should:Initiate incident response procedures.Consider reporting compromises immediately to applicable cybersecurity authorities.

4. Evaluate and apply other mitigations.

A. Remain alert to changes from vendors for the software on the asset, and immediately apply updates to assets when notified by a vendor that their product has a patch for this vulnerability.

B. Continue to monitor Log4J assets closely.

C. Continue to monitor the [Apache Log4j Security Vulnerabilities](https://logging.apache.org/log4j/2.x/security.html) webpage for new updates.

D. Block specific outbound Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) network traffic.

**To ensure advisory was actioned we are going to:**

provide training to employees who will be applying this advice. This will help them understand the logic behind the advice and how to apply it effectively.

Assign responsibility for applying the advice to specific individuals or teams within the company. This will help ensure that everyone knows who is responsible for implementing the advice and who to turn to if they have questions or concerns.

Regularly monitor the progress of the implementation to ensure that the advice is applied effectively.

**Provide** support and resources to help employees apply the advice.

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

Kind regards,  
AIG Cyber & Information Security Team