**From:** AIG Cyber & Information Security Team  
**To:**Product Development Team  
**Subject:** Security Advisory concerning Product Development Staging Environment Log4j Vulnerability

**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 your Product Development Staging Environment.

**Vulnerability Description**: The Log4j vulnerability allows unauthenticated remote actors to execute arbitrary code on systems using the affected versions of Log4j. This is due to improper input validation within the logging library, which can be exploited by sending specially crafted log messages.

**Vulnerability Risk/Impact**: This vulnerability's impact is critical as it can lead to full system compromise. An attacker can gain control over the affected system, potentially leading to data breaches, unauthorized access, and further exploitation within the network. Given the widespread use of Log4j, this vulnerability poses a significant threat to your staging environment and any connected systems.

**Vulnerability Remediation**: To mitigate this vulnerability, please take the following steps immediately:

* *Identify and Enumerate*: Identify all instances of Log4j within your environment.
* Apply Patches: Upgrade Log4j to the latest version immediately.
* Temporary Mitigations: If a patch is not available, apply the recommended mitigations such as removing the JNDI class from the classpath or setting system properties to disable JNDI lookups.
* Monitor and Scan: Continuously monitor your systems for any unusual activity and set up alerts for probes or attacks on devices running Log4j.
* Incident Response: Initiate hunt and incident response procedures to detect possible exploitation of the vulnerability.

**Assurances**: Please confirm that the above actions have been taken by sending a status update to the Cyber & Information Security Team. This will help us ensure that the advisory has been actioned and that your environment is secure.

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

Kind regards,  
AIG Cyber & Information Security Team