Email Created

From: AIG Cyber & Information Security Team
To: product@email.com

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.

The vulnerability, known as "Log4Shell" (CVE-2021-44228), is a critical flaw in the Apache Log4j logging library. This vulnerability allows an attacker to execute arbitrary code on any system using Log4j by manipulating log messages. Additional vulnerabilities, CVE-2021-45046 and CVE-2021-45105, have also been identified, compounding the risk.

Exploiting these vulnerabilities can allow attackers to gain full control over affected systems, leading to potential data breaches, system takeovers, and further malicious activity. Given the widespread use of Log4j, this vulnerability poses a significant threat to our infrastructure and must be addressed urgently.

Subject: Urgent Action Required: Log4j Vulnerability Remediation

Remediation Steps To Take:

Identify & Patch: Locate all Log4j instances and apply the latest Apache security patches immediately. If patching is delayed, use recommended workarounds to mitigate risk.
Review & Monitor: Conduct a thorough security review of Log4j-based systems and continuously monitor for exploitation attempts. Respond promptly to any incidents.

We'll train all team members on the vulnerability and implemented mitigation strategies.

Regular reports detailing identified Log4j instances, patched systems, and ongoing measures will be sent to the AIG Cyber & Information Security Team.

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

Kind regards,
AIG Cyber & Information Security Team