From: AIG Cyber & Information Security Team
To: Product Development Team (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 the Product Development Staging Environment infrastructure in your team.

Vulnerability Overview
Log4j is a library that is widely used for logging and monitoring Java-based applications. Recently, a vulnerability with this library (also known as Log4Shell) has been identified in versions Log4j2 2.0-beta9 through 2.15.0. Attackers can inject malicious codes into the log, hence performing remote code execution to take over the system.
NVD - CVE-2021-44228 and NVD - CVE-2021-45046.

Additional information:
CVE-2021-44228
CVE-2021-45046
CVE-2021-45105
CISA First Advisory
CISA Second Advisory

Affected products
Log4j2 2.0-beta9 through 2.15.0

Risk & Impact
Critical - Since the library is widely used across industries, a great number of attempted exploits have been reported. Hence, we recommend you fix the system as soon as possible to protect the Product Development Environment infrastructure.

Recommended Remediation

- Identify running assets affected by the Log4j version. Use this Github page
- Update the Log4j to the latest version (ie 2.16.0 for Java 8 & 2.12.2 for Java 7)
- Conduct vulnerability assessment to identify any potential exploits.
- Continue to monitor the applications for any signs of exploitations.

Please let us know if you have any questions or concerns regarding this vulnerability.

Kind regards,
AIG Cyber & Information Security Team