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

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

Vulnerability Description:

The vulnerability, known as Log4Shell, is tracked under CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105. These vulnerabilities affect versions of Apache Log4j 2 and allow unauthenticated remote code execution (RCE) via specially crafted log messages. These vulnerabilities are being exploited by threat actors, including those behind known ransomware operations.

Vulnerability Risk/Impact:

Successful exploitation could lead to complete system compromise, including the deployment of ransomware, data exfiltration, and disruption of services. These vulnerabilities have impacted organizations globally and have been highlighted in joint advisories from CISA, FBI, NSA, and allied international cybersecurity authorities.

Vulnerability Remediation:

Immediate remediation steps include:

- Upgrade to Log4j version 2.17.1 or later.
- For systems where upgrading is not immediately possible, follow temporary mitigation guidelines published by Apache and validated by CISA.
- Conduct forensic reviews and threat hunting activities to detect signs of compromise.
- Implement strict outbound network controls to block suspicious LDAP/RMI traffic.

Please ensure the relevant product and engineering teams evaluate their systems for the use of Log4j and apply patches or mitigations accordingly. We are tracking patch

compliance and mitigation status across affected environments. If this advisory has already been implemented, no further response is required at this time.

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

Kind regards,
AIG Cyber & Information Security Team