Example Email

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.

Vulnerability Overview
Log4j is a common open-source tool used for application logging and monitoring across the web. Recently, a vulnerability has been identified in versions Log4j2 2.0-beta9 through 2.15.0 that would allow an unauthenticated attacker to perform remote code execution on affected infrastructure, making this a critical vulnerability. You can learn more in the NIST disclosures: NVD - CVE-2021-44228 and NVD - CVE-2021-45046.

Affected products
Log4j2 2.0-beta9 through 2.15.0

Risk & Impact
Critical - remote code execution (RCE). An attacker will be able to remotely access the Product Development Staging Environment infrastructure to exfiltrate data or execute malicious actions.

Remediation

- Identify any assets or infrastructure running the affected Log4j version
- Update to the following versions: Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7)
- Be on the lookout for any signs of exploitation

If you identified any signs of exploitation, please immediately reach out. After you have remediated this vulnerability, please confirm with the security team by replying to this email.

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

Kind regards,
AIG Cyber & Information Security Team