From: AIG Cyber & Information Security Team
To: John Doe (product@email.com)
Subject: Security Advisory concerning Product Development Staging Environment - Log4j
—
Body:
Hello John,

The AIG Cyber & Information Security Team would like to inform you of a critical vulnerability recently discovered in the Apache Log4j logging framework that affects the Product Development Staging Environment.

vulnerability description

The Log4j vulnerability (CVE-2021-44228) allows unauthenticated remote code execution (RCE) by sending a specially crafted request to a system using Log4j. This exploit leverages the framework's logging feature to inject malicious code, potentially compromising the affected system.

risk/impact

This vulnerability is classified as critical (CVSS score: 10.0) and poses severe risks, including:

- Full system compromise.
- Unauthorized access to sensitive data.
- The possibility of the staging environment being leveraged as a pivot point for further attacks within the infrastructure.

vulnerability remediation

Immediate action is required to mitigate this vulnerability:

1. **Update Log4j**: Upgrade to version 2.15.0 or later, where the vulnerability has been patched.
2. **Temporary Mitigation (if updating is not immediately possible)**:
    - Set the log4j2.formatMsgNoLookups system property to true.
    - Remove the JndiLookup class from the classpath by running:

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

1. Review and monitor logs for any signs of exploitation.
2. Conduct a thorough security assessment of the affected environment post-remediation.

Action Required

Please confirm the completion of the above steps or share any challenges you encounter in addressing this issue.

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

Kind regards,
AIG Cyber & Information Security Team