Email Task

Draft your advisory email below

To finish this task, draft an advisory email to alert the infrastructure owner of the seriousness of this vulnerability.

For inspiration, you can use the email template provided below from our last cyber threat advisory.

> **From:** AIG Cyber & Information Security Team
> **To:** <affected team>
> **Subject:** Security Advisory concerning <affected product> <affected software>
> —
> **Body:**
> Hello <affected team owner>,
>
> AIG Cyber & Information Security Team would like to inform you that a recent <affected software> vulnerability has been discovered in the security community that may affect <affected product>.
>
> <vulnerability description>
>
> <vulnerability risk/impact>
>
> <vulnerability remediation>
>
> <any assurances to ensure advisory was actioned>
>
> For any questions or issues, don't hesitate to reach out to us.
>
> Kind regards,
> AIG Cyber & Information Security Team

Tips for your email:

- Make it direct and straight to the point.
- You can assume the infrastructure owner is technical.
- Explain the risk/impact, method of exploitation, and remediation steps.

My Response

From: AIG Cyber & Information Security Team
To: Product Development Team (product@email.com)
Subject: Urgent Security Advisory: Apache Log4j Vulnerability Affecting Product Development Staging Environment

Hello John Doe,

The AIG Cyber & Information Security Team needs to inform you of a critical vulnerability recently discovered in Apache Log4j that may affect the Product Development Staging Environment.

Vulnerability Overview
A severe vulnerability (CVE-2021-44228) has been identified in Apache Log4j versions 2.0-beta9 through 2.15.0. This flaw allows remote code execution (RCE) via crafted log messages, posing a high risk if exploited. This vulnerability impacts systems using these versions of Log4j for logging and monitoring.

Risk & Impact
The impact is classified as critical due to the potential for remote code execution. Attackers could exploit this vulnerability to gain unauthorized access, execute arbitrary commands, and compromise the Product Development Staging Environment.

Remediation Steps

1. **Assess**: Identify and verify any systems using the affected versions of Log4j within the Product Development Staging Environment.
2. **Update**: Upgrade Log4j to version 2.17.1 or later to address this vulnerability.
3. **Mitigate**: As a temporary measure, you can disable JNDI (Java Naming Directory Interface) lookups by setting the system property log4j2.formatMsgNoLookups to true.
4. **Monitor**: Implement additional monitoring to detect any unusual activity or signs of exploitation.

Please confirm receipt of this advisory and notify us once remediation actions have been taken. If you encounter any issues or require assistance, do not hesitate to reach out.

Thank you for your attention to this matter.

Kind regards,
AIG Cyber & Information Security Team