POS Digicert

**27 December 2021**

Dear Valued Customer,

## Apache Log4j 2 Vulnerability

Log4j2 is an open-source, Java-based logging framework commonly incorporated into Apache web servers. According to public sources, Chen Zhaojun of Alibaba officially reported a Log4j2 remote code execution (RCE) vulnerability to Apache on November 24, 2021. The log4j security vulnerability allows attackers to execute malicious code remotely on a target computer. Meaning, bad actors (hackers) can easily steal data, install malware, or simply take control of a system via the Internet.

Pos Digicert is actively following the security vulnerabilities in the open-source Apache “Log4j 2" utility (CVE-2021-44228). Based on our findings, Pos Digicert’s core services for its customers are not using Log4j 2 and are **NOT IMPACTED** by the issues identified in CVE-2021-44228.

## Summary

A critical vulnerability in Apache Log4j2 (CVE-2021-44228) has been publicly disclosed that may allow for remote code execution, impacting products that use the library. After a comprehensive audit, all POS DIGICERT SDN BHD’s product and cloud/roaming services are not impacted by this vulnerability.

## Date of Publication

27 Dec 2021

## Description

This vulnerability only affects log4j versions between 2.0 and 2.14.1. The exploit requires an attacker to remotely access an endpoint and send arbitrary data logged or otherwise processed by the log4j engine. Once the vulnerability was identified, Pos Digicert completed a comprehensive audit of all its software and services, and our infrastructure team has established that Pos Digicert’s users are not impacted by the critical Apache Log4j vulnerability known as CVE-2021-44228.

Based on our infrastructure team’s audit, there is no additional remediation required for any Pos Digicert Software or Service at this time.

Related to this incident, here are additional specifics for the Pos Digicert's software, services portfolio and any action that is required.

| Software/Service | Description | Impact Statement | Action Required |
|---|---|---|---|
| **Pos Digicert Document Signing Solutions (DSS)** | Software used to digitally signs softcopy documents. | The solution does not use the affected library at this time. So, it is not exposed to this vulnerability. | None Required |
| **Pos Digicert iVest Server** | Service used to validate certificates by referring to certificate expiry date, certificate integrity and revocation. | The solution does not use the affected library at this time. So, it is not exposed to this vulnerability. | None Required |
| **Pos Digicert BizClient** | Service used to protect access and establishes secure connection for transactions in business-to-business (B2B) environment over the internet. | The solution does not use the affected library at this time. So, it is not exposed to this vulnerability. | None Required |
| **Pos Digicert iFile** | Service used to protect File confidentiality and origin authentication, and to preserve data | This service does not use the reported library and thus is not vulnerable to it. | None Required |

| | | | |
|---|---|---|---|
| | integrity and non-repudiation; which are the four core security goals. | | |
| **Pos Digicert eCredentia** | Service used in managing records including transcripts, certificates and official letters to be digitally signed | This service does not use the reported library and thus is not vulnerable to it. | None Required |

**References**

CISA - https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
CVE - https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228
Apache - https://logging.apache.org/log4j/2.x/security.html

As always, if you have any questions after reviewing this update please do not hesitate to reach out to us directly at customercare@posdigicert.com.my.

Thank you for being a valued Pos Digicert customer.

Regards,

The Management of Pos Digicert Sdn Bhd