RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Direction générale des douanes et droits indirects

BP3X24V1

CONCOURS EXTERNE ET INTERNE

POUR LE RECRUTEMENT DE CONTRÔLEURS DES DOUANES ET DROITS INDIRECTS

BRANCHE DU CONTRÔLE DES OPÉRATIONS COMMERCIALES ET D'ADMINISTRATION GÉNÉRALE

SPÉCIALITÉ « TRAITEMENT AUTOMATISÉ DE L'INFORMATION – PROGRAMMEUR »

SESSION 2024

ÉPREUVE ÉCRITE D'ADMISSION N°3

(DURÉE : 1 HEURE 30 MINUTES– COEFFICIENT 1)

TRADUCTION D'UN TEXTE EN ANGLAIS ISSU D'UNE REVUE OU D'UNE DOCUMENTATION INFORMATIQUE

AVERTISSEMENTS IMPORTANTS

Veillez à bien paginer vos copies.

L'usage de tout matériel autre que le matériel usuel d'écriture et de tout document autre que le support fourni est **interdit**.

La copie ne saurait comporter de **nom, initiales, paraphe, signature, lieu géographique ou tout autre signe distinctif**, susceptibles de permettre l'identification du candidat. Le non-respect de cette consigne entraînera l'exclusion du concours.

Toute fraude ou tentative de fraude constatée par la commission de surveillance entraînera **l'exclusion du concours.**

Il vous est interdit de quitter définitivement la salle d'examen **avant le terme de l'épreuve**.

Le présent document comporte **3 pages** numérotées.

What Is Apache Log4J (Log4Shell) Vulnerability?

Log4Shell vulnerability overview

2021 was a busy year for zero-day vulnerabilities capped off by Log4Shell, a critical flaw found in the widely used Java-based logging library, Apache Log4j. Officially identified as CVE-2021-44228, it carries a severity score of 10 out of 10 (CVSS v3.1) from the Common Vulnerability Scoring System (CVSS).

The vulnerability was first privately reported to Apache on Nov. 24, 2021. On Dec. 9, 2021 Log4Shell was publicly disclosed and initially patched with version 2.15.0 of Apache Log4j.

Subsequent news of observed attacks in the wild triggered several national cybersecurity agencies to issue warnings, including the US Cybersecurity and Infrastructure Security Agency (CISA), UK National Cyber Security Center (NCSC), and Canadian Center for Cyber Security. Due to the popularity of Apache Log4j, hundreds of millions of devices could be impacted.

How Log4Shell works

Log4Shell is a Java Naming and Directory Interface™ (JNDI) injection vulnerability which can allow remote code execution (RCE). By including untrusted data (such as malicious payloads) in the logged message in an affected Apache Log4j version, an attacker can establish a connection to a malicious server via JNDI lookup. The result: full access to your system from anywhere in the world.

Since JNDI lookup supports different types of directories such as Domain Name Service (DNS), Lightweight Directory Access Protocol (LDAP) which provide valuable information as the organization's network devices, remote method invocation (RMI), and Inter-ORB Protocol (IIOP), Log4Shell can lead to other threats such as:

- Coinmining: Attackers can use your resources to mine cryptocurrency. This threat can be quite costly, given vast amount of computing power required to run services and applications in the cloud.
- Network denial of service (DoS): This threat allows attackers to shut down and/or disable a network, website, or service so it is inaccessible to the targeted organization.
- Ransomware: After RCE is achieved, attackers can collect and encrypt data for ransom purposes.

[…]

Vulnerable products, applications, and plug-ins

Essentially, any internet-facing device running Apache Log4j versions 2.0 to 2.14.1. The affected versions are included in Apache Struts, Apache Solr, Apache Druid, Elasticsearch, Apache Dubbo, and VMware vCenter.

Patch and mitigation

Apache initially released Apache Log4j version 2.15.0 to patch the vulnerability. However, this version only worked with Java 8. Users of earlier versions needed to apply and re-apply temporary mitigations. At the time of publication, Apache released version 2.16.0 and advised users to update their potentially affected library as quickly as possible.

Other mitigation strategies such as virtual patching and utilizing an intrusion detection/prevention system (IDS/IPS) are strongly encouraged. Virtual patching shields the vulnerability from further exploitation, while IDS/IPS inspects ingress and egress traffic for suspicious behavior.

Source : https://www.trendmicro.com/en_ae/what-is/apache-log4j-vulnerability.html

November 6, 2023