CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

TLP:WHITE

******
ALERTE
******

Numéro : AL21-019 – MISE À JOUR 1
Date : 10 décembre 2021
Mise à jour : 11 décembre 2021

****
Exploitation active de la vulnérabilité Apache Log4j
****

AUDITOIRE
=========
La présente alerte s'adresse aux professionnels et aux gestionnaires des TI œuvrant au sein des organismes avisés. Les destinataires de la présente information peuvent redistribuer celle-ci au sein de leurs organismes respectifs.

OBJET
=====
Une alerte a pour objet de prévenir les destinataires que des cybermenaces ont été relevées récemment et que celles-ci pourraient toucher les biens d'information électronique. Elle vise également à leur fournir des conseils supplémentaires en matière de détection et d'atténuation. Au reste, le Centre canadien pour la cybersécurité (ou Centre pour la cybersécurité) est en mesure d'offrir, aux destinataires qui en font la demande, une assistance complémentaire concernant la teneur de la présente alerte.

VUE D'ENSEMBLE
==============
Le 10 décembre 2021, Apache a publié un bulletin de sécurité [1][2] soulignant une vulnérabilité critique menant à l'exécution de code à distance liée au produit Log4j, un outil de journalisation JAVA largement déployé. Selon des rapports de sources ouvertes, des cas d'exploitation et de balayage actifs ont été observés.

DÉTAILS
=======
Le 10 décembre 2021, Apache a publié un bulletin de sécurité [1][2] soulignant une vulnérabilité critique menant à l'exécution de code à distance liée au produit Log4j, et touchant les versions 2.0-beta9 à 2.14.1. Un auteur de menace non authentifié distant pourrait exploiter cette vulnérabilité pour exécuter du code arbitraire sur l'appareil touché.

Selon des rapports de sources ouvertes, des cas d'exploitation et de balayage actifs de la vulnérabilité (désignée CVE-2021-44228 [3]) ont été observés. En raison de l'utilisation répandue de la bibliothèque Log4j dans des infrastructures populaires, de nombreuses applications de tierces parties pourraient être vulnérables à une tentative d'exploitation. Log4j est aussi souvent utilisé dans les logiciels Java d'entreprise, et est intégré dans plusieurs infrastructures Apache, y compris les suivantes (sans s'y limiter) : Apache Struts2, Apache Solr, Apache Druid, Apache Flink et Apache Swift. Log4j est aussi intégré dans la bibliothèque d'autres infrastructures Java, y compris (sans s'y limiter : Netty, MyBatis et Spring. [4]

MISE À JOUR 1

La bibliothèque Apache Log4j permet aux développeurs de consigner les résultats tirés des différentes sources de données dans leurs applications. Dans certains cas, les données consignées proviennent d'entrées utilisateur. Elles prennent notamment en charge les fonctions de Java Naming and Directory Interface (JNDI), qui sont utilisées dans la configuration, les messages de journalisation et les paramètres. Dans le cas des versions vulnérables de Log4j, les données d'utilisateurs consignées qui contiennent des recherches JNDI vers des points d'extrémité contrôlés par un auteur de menace pourraient permettre à ce dernier de charger du code arbitraire sur le serveur afin de l'exécuter depuis le point d'extrémité.

Le Centre pour la cybersécurité recommande fortement aux organisations de passer en revue en interne les applications potentiellement touchées. Bien qu'elles ne soient pas exhaustives, les sources communautaires facilitent les efforts déployés pour identifier les produits touchés. [8]

Apache a publié la version 2.15 du produit Log4j, qui corrige cette vulnérabilité. De plus, Apache a fourni pour les versions précédentes des solutions de contournement à appliquer si une mise à niveau n'est pas possible.

MESURES RECOMMANDÉES

Le Centre pour la cybersécurité recommande aux organisations qui utilisent des applications avec Apache Log4j de faire ce qui suit :

- mettre à niveau leurs applications à la version 2.15.0 de Log4j si possible;
- appliquer les solutions de contournement proposées par Apache si elles ne peuvent faire la mise à niveau immédiatement;
- vérifier les journaux afin de détecter tout indice de compromission.

Les autres fournisseurs touchés par les vulnérabilités signalées pourraient aussi publier des bulletins de sécurité liés à leurs produits.

DÉTECTION

Identifier les recherches Java Naming and Directory Interface (JNDI) dans les journaux en amont afin de détecter toute tentative d'exploitation ou d'évaluer toute incidence éventuelle. [5][6]

Vérifier le trafic provenant d'adresses IP connues [7] en consultant les journaux du pare-feu.

MISE À JOUR 1

ATTÉNUATION
==========

Apache recommande de prendre les mesures d'atténuation suivantes s'il est impossible d'appliquer les correctifs immédiatement : [1]

- Dans les versions 2.10 et ultérieures de Log4j, on peut atténuer le comportement vulnérable en réglant la propriété "log4j2.formatMsgNoLookups" à "true". La variable d'environnement "LOG4J_FORMAT_MSG_NO_LOOKUPS" peut également être définie à "true" afin de minimiser ce comportement.
- Dans les versions 2.0-beta9 à 2.10.0 de Log4j, la mesure d'atténuation consiste à supprimer la classe JndiLookup dans l'élément Classpath en exécutant la commande suivante :
  - "zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class"

On invite les destinataires à communiquer avec le Centre pour la cybersécurité par l'entremise de Mon cyberportail (https://cyber.gc.ca/fr/cyberincidents), par courriel (contact@cyber.gc.ca) ou par téléphone (1-833-CYBER-88 ou 1-833-292-3788), s'ils relèvent des activités similaires à ce qui est présenté dans la présente alerte.

RÉFÉRENCES
==========

[1] Apache Log4j Advisory
https://logging.apache.org/log4j/2.x/security.html (anglais seulement)

[2] Bulletin de sécurité Apache AV21-626 du Centre pour la cybersécurité
https://www.cyber.gc.ca/fr/avis/bulletin-de-securite-apache-3

[3] CVE-2021-44228
https://nvd.nist.gov/vuln/detail/CVE-2021-44228 (anglais seulement)

[4] CERT United Kingdom Alert: Active scanning for Apache Log4j 2 vulnerability (CVE-2021-44228)
https://www.ncsc.gov.uk/news/apache-log4j-vulnerability (anglais seulement)

[5] CERT New Zealand - Log4j RCE 0-day actively exploited
https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively exploited/ (anglais seulement)

[6] Florian Roth - log4j RCE Exploitation Detection (Grep and YARA)
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b (anglais seulement)

[7] Greynoise - IP List - CVE-2021-44228 Apache Log4j RCE Attempts
https://gist.github.com/gnremy/c546c7911d5f876f263309d7161a7217 (anglais seulement)

[8] Ressources communautaires GitHub identifiant les applications vulnérables
https://github.com/YfryTchsGD (anglais seulement)

NOTE AUX LECTEURS
==========

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) mène ses activités sous l'égide du Centre de la sécurité des télécommunications. Il constitue l'autorité canadienne en matière de cybersécurité et dirige les interventions du gouvernement lors d'événements liés à la cybersécurité. Le personnel du Centre pour la cybersécurité agit à titre d'équipe nationale d'intervention en cas d'incident lié à la sécurité informatique et travaille étroitement avec les ministères, les propriétaires et exploitants d'infrastructures essentielles, les entreprises canadiennes et des partenaires internationaux pour intervenir en cas d'incident de cybersécurité ou pour atténuer les conséquences qui en découlent. C'est dans cette optique que nous prodiguons des conseils d'experts et offrons un soutien de premier plan, et que nous coordonnons la diffusion de l'information pertinente ainsi que les interventions en cas d'incident. Le Centre pour la cybersécurité est à l'écoute des entités externes et favorise les partenariats visant à créer un cyberespace canadien fort et résilient.