HISCOX
CYBERCLEAR®

Rapport d'incident de sécurité
Communication destinée aux courtiers
14 décembre 2021

Exploitation récente de Java Log4j : Que devez-vous savoir et dire à vos clients ?

Temps de lecture 2 minutes

Jeudi 9 décembre 2021, un *exploit zero-day* (programme d'exploitation d'une faille inconnue) de la librairie de logging Java Log4j a été identifié. Il s'agit d'une librairie communément utilisée pour créer et stocker des informations de logging de logiciels, applications, équipements informatiques etc.

Les versions concernées de Log4j sont 2.0 - 2.14.1, la vulnérabilité est corrigée dans la version 2.15.0

Quelle est l'ampleur du risque ?

Il s'agit d'une vulnérabilité particulièrement dangereuse parce que l'exploitation peut être réalisée à distance, qu'elle ne requiert pas d'authentification et qu'elle peut donner accès intégralement au serveur ou à l'appareil attaqué. De plus, son exploitation est simple (une simple ligne de code suffit) et des exemples d'attaques sont d'ores et déjà publiés en ligne.

Cette librairie de logging est largement utilisée et on la trouve dans un grand nombre d'équipements et de logiciels d'entreprises comme Apache Struts et Tomcat, Solr, distributions Linux, Blackberry Symantec, Apple etc.

Qui est le plus touché ?

Malheureusement, il n'y a pas de type d'entreprise susceptible d'être plus affectée qu'une autre et il est difficile pour une entreprise de savoir si elle est vulnérable. Par exemple, un de vos clients pourrait très bien ne pas avoir la vulnérabilité dans la version du logiciel qu'il a programmée, mais il est tout à fait possible que des équipements qu'il exploite (comme les périphériques VPN, les fournisseurs de cloud etc.) puissent contenir la vulnérabilité.

Comme il s'agit d'une librairie Apache, il est plus probable qu'elle fonctionne sur des serveurs Linux, néanmoins, c'est une vulnérabilité Java et Java peut fonctionner sur de multiples plateformes. Ainsi, les serveurs Windows, Linux et Apple pourraient tous être vulnérables. Nous estimons que les entreprises dont la valeur est comprise entre 25 millions et 1 milliard £/$/€ sont les plus à risque, car elles sont susceptibles d'exploiter des logiciels/appareils vulnérables, elles peuvent avoir les compétences ou les connaissances pour corriger la vulnérabilité.

Que devez-vous dire à vos clients ?

Les questions essentielles à poser à vos clients :

- Êtes-vous au courant de la nouvelle vulnérabilité log4j également dénommée CVE-2021-44228 ou log4shell ?
- Avez-vous évalué votre risque au regard de cette vulnérabilité pour les applications développées en interne ?
- Avez-vous contacté vos fournisseurs d'équipements/de logiciels/de cloud et vérifié si leurs services sont impactés ?
- Avez-vous un plan d'action en déploiement et à déployer pour prévenir de ce risque et traiter les points ci-dessus ?

Apache a publié ici une note de sécurité pour traiter cette vulnérabilité et mis en ligne un correctif pour y remédier (2.15.0).

Pour en savoir plus (veuillez noter qu'il s'agit de liens externes qui ne sont ni validés ni vérifiés par Hiscox) :

- Publications de l'ANSSI relatives à ce sujet : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
- Précisions complémentaires de Lunasec.
- Liste de plus de 180 fournisseurs avec des liens vers leurs instructions (compilée par un chercheur français en cybersécurité).