Vulnérabilité Log4j : une nouvelle alarmante pour les créateurs et les consommateurs de services numériques

11 janvier 2022, 01:00

Tatiana Galibus

La fin de décembre 2021 a apporté des nouvelles alarmantes pour les entreprises de services numériques du monde entier, en raison de la découverte d'une vulnérabilité critique dans la bibliothèque Apache Log4j. Cette bibliothèque open source est largement utilisée pour consigner des informations relatives à la sécurité et aux performances. Log4j fait donc partie intégrante des services et des applications grand public et professionnelles. Malheureusement, elle se rencontre également dans les entreprises manufacturières, car elle est largement utilisée dans les produits technologiques opérationnels.

Qui est concerné ?

Tout service et application utilisant la bibliothèque de journalisation Java, Apache Log4j (CVE-2021-44228), entre les versions 2.0 et 2.15. Ceci comprend des services comme **Atlassian, Amazon, Microsoft Azure, Cisco, Fortinet, Oracle, Red Hat, Splunk, Soft et VMware**.

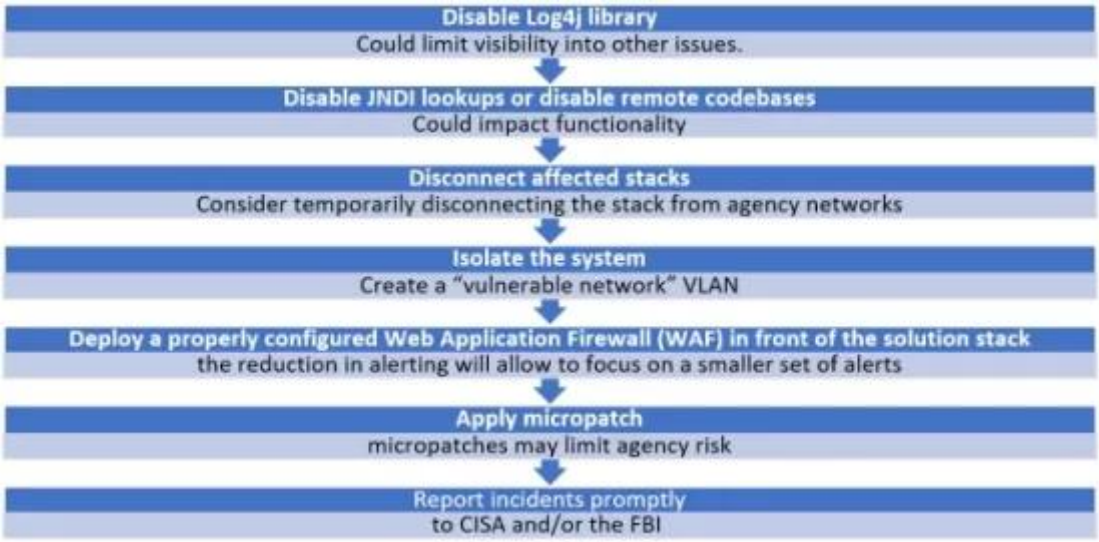
Cette bibliothèque est donc présente dans la majorité des applications et des sites web populaires, et des centaines de millions d'appareils de par le monde qui accèdent à ces services sont potentiellement exposés à cette vulnérabilité.

Avec quel impact ?

Comme il s'agit d'une vulnérabilité de type « zero-day », Log4j permet à des parties malveillantes d'exécuter n'importe quel code à distance, que ce soit via un LAN, un WAN ou internet. **En outre, elle peut être exploitée en peu de temps**. La vulnérabilité affecte **le traitement des messages de journal**. Un auteur de menaces peut amener le système à charger du code externe simplement en envoyant un message conçu à cet effet (exécution de commande à distance).

L'élément le plus alarmant concernant ces attaques est qu'il faudra peut-être aux petites entreprises des années pour remédier à cette vulnérabilité, alors que de leur côté, les pirates cherchent constamment de nouvelles façons de l'exploiter. Ils pourraient très bientôt l'utiliser pour des attaques plus sophistiquées afin d'obtenir des gains plus importants. Dans un avenir proche, elle pourrait devenir une véritable bombe à retardement.

Comment y remédier ?



Les rapports peuvent être envoyés ici. Consultez cette page pour rester au courant des mesures d'atténuation.

Et ensuite ?

« Ce qui m'inquiète le plus, ce sont les districts scolaires, les hôpitaux, les endroits où un seul informaticien s'occupe de la sécurité et n'a pas le temps, le budget ou les outils nécessaires à la sécurité », explique Katie Nickels, iDirector of Intelligence dans la société de cybersécurité Red Canary. *« Ce sont les organisations qui m'inquiètent le plus, les petites organisations qui ont des budgets de sécurité restreints. »*

Malheureusement, le traitement de ces vulnérabilités de la chaîne d'approvisionnement nécessite souvent des analyses de sécurité par des tierces parties et des compétences en matière de détection d'incidents. Comment sensibiliser efficacement et faire face à Log4j ou à une autre vulnérabilité critique dans le logiciel que vous utilisez au quotidien ? La meilleure façon consiste à apprendre à se protéger et à réagir intelligemment ! Sirris et Agoria peuvent vous y aider : apprenez la cybersécurité d'une manière appliquée et pragmatique dans plusieurs de nos masterclasses ! Toutes les formations sont subventionnées par VLAIO, de sorte que les entreprises de Flandre ne paient que 30 %.

Auteurs



Tatiana Galibus