Log4Shell : un expert détaille les dangers de la faille de sécurité pour les entreprises

Derrière le nom complexe de Log4Shell se trouve une faille de sécurité qui inquiète les spécialistes de la cybersécurité. Cette dernière touche un petit module de code en accès libre, utilisé dans de très nombreux logiciels et applications à travers le monde. Voici pourquoi les entreprises doivent prendre des dispositions d'après David Sygula, head of threat investigation à CybelAngel.

Temps de lecture : minute

20 décembre 2021

"*C'est à la fois un sprint et un marathon pour les sociétés à travers le monde qui démarre.*" David Sygula, head of threat investigation à CybelAngel, ne mâche pas ses mots quand il évoque la menace de la faille Log4Shell qui plane depuis début décembre 2021 sur toutes les organisations. Comme l'Agence nationale pour la sécurité des systèmes d'information (Anssi) le relevait mi-décembre, cette vulnérabilité affecte Log4j. Ce petit module de code en accès libre est utilisé dans de très nombreux logiciels et applications dans le monde, et notamment dans des serveurs – ce qui explique le fait qu'il concerne autant d'acteurs. CybelAngel, startup membre du Next40 et experte de la cybersécurité, alerte notamment quant à "*la rapidité de la militarisation*" de cette faille récente créée par les pirates informatiques. Ce qui constituerait donc sa "*différence avec les autres grandes failles des derniers mois*".

Ne pas se contenter de la mise à jour

Son homologue américaine HackerOne relève que les signalements de vulnérabilités liées à ce Log4j ont été multipliées par 140 en une semaine, entre le 9 et le 16 décembre 2021. "*Depuis plusieurs jours, des preuves de concept* (PoC) *actionnables sont échangées au sein des communautés cybercriminelles. Divers groupes de ransomware* [rançongiciel] *ont ajouté la faille à leur arsenal, et de nombreuses utilisations ont été répertoriées*" , confirme David Sygula, arguant de ce fait que "*nous n'avons pas fini d'en entendre parler*". Sachant que tester massivement l'exploitation de cette vulnérabilité est plus simple et rapide pour les cybercriminels que de l'identifier et de la colmater pour les entreprises, la crise prend de grandes proportions.

L'Anssi a ainsi appelé les organisations à remédier à la situation en appliquant la mise à jour officielle du module Log4j. Mais là n'est pas la seule action à entreprendre si l'on en croit CybelAngel, qui appelle également à réaliser un état des lieux.

À lire aussi

Covid-19 : Comment CybelAngel a neutralisé une escroquerie visant un fabricant de vaccins

David Sygula indique qu'il est "*recommandé de dresser l'inventaire des services touchés, au-delà de mettre à jour au plus vite vers la dernière version de l'utilitaire*". Une partie qu'il qualifie de "*sprint*" , qui ne représente en soi pas une mince affaire : "*Log4j est une petite brique. Elle peut passer inaperçu aux yeux des services de maintenance, sans compter le fait qu'il existe de nombreux utilitaires concurrents.*"

Une faille découverte sur le jeu vidéo Minecraft

Le spécialiste de la cybersécurité mise également sur un "*marathon*" , pour lutter dans le temps contre la vulnérabilité. "*Il convient de disposer de solutions de protection proactives, qui permettent d'enrayer la kill chain* [la chaîne de frappe est une méthode de modélisation des procédés d'intrusion sur un réseau informatique, N.D.L.R.] " , pointe David Sygula, qui note également qu'un "*système robuste avec des permissions et droits corrects limite la casse*". Log4Shell ne fait pas exception.

L'Anssi, qui indiquait dans un communiqué diffusé en fin de semaine dernière n'avoir "*constaté que des attaques relativement bénignes*" , alertant en même temps que cela "*ne présage en rien des exploitations futures ou encore non détectées*" – et potentiellement plus graves. Erwan Keraudy, co-fondateur et président-directeur général de CybelAngel, nous a confié que la faille a été "*découverte pas des personnes qui testaient* [un procédé] *sur le jeu vidéo Minecraft*".

Une anecdote jugée "*savoureuse*" par le dirigeant, qui rappelle que les hackers ne perdent pas de temps : "*C'est fascinant de voir combien les attaquants bougent vite.*" Microsoft a notamment rapporté que des

organisations de cyberespionnage chinoises, iraniennes, nord-coréennes et turques ont d’ores et déjà exploité la faille, qui a été classée au niveau maximum dans l’échelle de criticité des vulnérabilités. C’est une des raisons pour lesquelles Erwan Keraudy juge que cela en fait "*la mère de toutes les failles*".

Article écrit par Arthur Le Denn