L'Anssi presse les organisations de remédier à la faille de sécurité Log4Shell

L'Anssi alerte les organisations quant à la gravité de la faille de sécurité "Log4Shell" . Elle enjoint les directions des systèmes d'information à la colmater en appliquant une mise à jour officielle du module à l'origine de la vulnérabilité. Les cybercriminels ayant pris de l'avance, des vols de données ne sont pas à écarter.

Temps de lecture : minute

16 décembre 2021

L'heure est à la réaction. L'Agence nationale pour la sécurité des systèmes d'information (Anssi) a pressé, ce jeudi 16 décembre 2021, les responsables informatiques d'organisations de remédier "*rapidement*" à la faille critique "Log4Shell" , rendue publique la semaine dernière et extrêmement répandue.

"*Pour l'instant, l'Anssi n'a constaté que des attaques relativement bénignes, ce qui ne présage en rien des exploitations futures ou encore non détectées, potentiellement bien plus graves*, a-t-elle indiqué dans un communiqué de presse. *Il est donc indispensable, pour les organisations, de mener rapidement un travail d'inventaire pour identifier leurs applications potentiellement vulnérables et procéder d'urgence aux mises à jour de sécurité.*"

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

De potentiels vols de données

La vulnérabilité en question affecte Log4j, un petit module de code en logiciel libre utilisé dans de très nombreux logiciels et applications à travers le monde, dans des serveurs. Des remèdes ont été publiés par l'éditeur, l'Apache Software Foundation, pour colmater la faille. Mais la difficulté, pour les responsables de sécurité informatique partout dans le monde, est de parvenir à identifier tous les programmes qui ont recours à ce petit module.

"*Log4j est embarqué dans de très nombreux logiciels, eux-mêmes déployés sur toutes sortes d'appareils, des serveurs web aux appareils connectés, et personne ne s'est vraiment préoccupé de sa présence jusqu'ici. Il faut donc descendre profondément dans les couches logicielles pour le voir*" , a indiqué à *La Tribune* Philippe Rondel, senior security architect pour le fournisseur israélien de services de sécurité

Check Point.

L'exploitation de la faille est simple, et peut permettre de prendre le contrôle du serveur concerné, ouvrant la porte à des attaques par rançongiciels, des vols de données ou des activités d'espionnage. L'Anssi conseille d'ailleurs préventivement aux entreprises et organisations de vérifier qu'ils disposent bien "*de sauvegardes à jour et conservées hors ligne*" , "*dans la perspective probable d'une exploitation rapide de cette faille*" dans des attaques au rançongiciels.

À lire aussi
Après deux ans d'attente, le Campus Cyber de la Défense ouvre enfin ses portes

Les cybercriminels ont pris de l'avance

D'après des observations des spécialistes américains Cisco et Cloudflare rapportées par *The Record*, média en ligne appartenant à l'entreprise américaine de cybersécurité Recorded Future, les premières traces de l'exploitation de Log4Shell datent du 1er décembre. Certains acteurs malveillants ont donc dix jours d'avance sur les défenseurs. Microsoft a

depuis rapporté que des organisations de cyberespionnage chinoises, iraniennes, nord-coréennes et turques ont exploité la faille. Un constat sort de ces premiers retours : tous les types d'acteurs, des plus petits aux plus avancés, s'intéressent à Log4Shell.

La simplicité d'exploitation est l'une des raisons pour lesquelles cette faille dans Log4j a été classée au niveau maximum (10) dans l'échelle de criticité des vulnérabilités. Cette dernière "*promet des fêtes de fin d'année un peu pénibles pour beaucoup d'experts*" , a estimé le directeur général de l'Anssi Guillaume Poupard, en allusion aux efforts pour identifier tous les endroits ou le module vulnérable est utilisé. Et Philippe Rondel d'ajouter, auprès de *La Tribune* : "*Si l'on compare la vulnérabilité Log4Shell à un tsunami, nous sommes encore dans la phase de séisme, et nous attendons la vague.*"

Maddyness avec AFP

Article écrit par Maddyness, avec AFP