CYBER DEFENSE AFRICA : ANNONCE SÉCURITÉ **Date** : 12/12/2021

Type de Contenu	Description
Titre	*Zero-day dans la bibliothèque Java Log4j*
ID	*202112/Alerte/01*
Code LTP	*White*
Niveau de Risque	*Elevé*
Application et service Affectés	*Ruide Apache, Apache Flinkn, Apache Solr, Apache Spark, Apache Struts2, Apache Tomcat*
Version	*2.0 et 2.14.1*
Plateforme	*Apache Struts*
Mise à jour	*Log4j-2.15.0-rc2*
Résumé	*Vulnérabilité permettant l'exécution de code à distance non authentifié et l'accès aux serveurs.*
Impacts	*Accès total aux serveurs affectés*
Description Détaillée	*La bibliothèque Apache log4j permet aux développeurs de consigner diverses données au sein de leur application. Dans certaines circonstances, les données enregistrées proviennent d'une entrée utilisateur. Si cette entrée utilisateur contient des caractères spéciaux et est ensuite enregistrée dans le contexte de log4j, la recherche de méthode Java sera finalement appelée pour exécuter la classe Java distante définie par l'utilisateur sur le serveur LDAP. Cela conduira à son tour à RCE sur le serveur victime qui utilise l'instance log4j 2 vulnérable.*
Solutions	*Il est de demandé de faire une mise à jour Log4j-2.15.0-rc2.* *Avec la publication du correctif officiel d'Apache, il a été initialement rapporté que 2.15.0-rc1 avait corrigé la vulnérabilité CVE-2021-44228. Cependant, un contournement ultérieur a été découvert. Une nouvelle version 2.15.0-rc2 a été publiée à son tour, qui protège les utilisateurs contre cette vulnérabilité.* *N.B : Log4j 2.15.0 nécessite Java 8 . Par conséquent, les organisations qui utilisent Java 7 devront effectuer une mise à niveau avant de pouvoir passer à la version corrigée de Log4j.*
Liens pour plus de détails	https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability