RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

MARS

***M**essage d'**A**lerte **R**apide **S**anitaire*

MINISTERE DES SOLIDARITES ET DE LA SANTE

SERVICE DU HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE

DATE : 16/12/2021 **REFERENCE :** MARS N°2021_51

OBJET : SENSIBILISATION « LOG4J »

Pour action

☒Établissements médico-sociaux ☒Établissements hospitaliers

Pour information

☒DGOS ☒ARS ☒SG

☒DGCS ☒ARS de Zone ☒SHFDS ☐Autre :

Mesdames, Messieurs,

Depuis le 9 décembre 2021, a été identifiée une faille numérique appelée « Log4j » (également connue sous le nom de "Log4Shell"). Il s'agit d'une **vulnérabilité majeure,** relativement simple à exploiter, **« cotée » 10/10** par l'organisme qui l'a référencé « CVE-2021-44228 ».
Par l'intermédiaire du CERT Santé et des contacts SSI des ministères sociaux, cette alerte, diffusée par l'ANSSI le 10 décembre, a été largement relayée dans les réseaux spécialisés SSI.
J'attire votre attention, sur le **caractère exceptionnel de cette faille**, le composant Log4j étant utilisé dans de nombreuses formes de logiciels commerciaux ou open source, notamment des plateformes cloud, des applications web et des services divers. Cette popularité signifie qu'un **très large éventail de logiciels pourrait être menacé** par des tentatives d'exploitation de la vulnérabilité.

C'est au regard de cette situation hors norme que j'ai souhaité attirer votre attention personnelle.

Selon nos informations, des cyber-attaquants analysent déjà les systèmes exposés sur Internet à la recherche d'instances vulnérables de Log4j pour y insérer différents « malware » dont des rançongiciels ». Cette faille pourrait aussi entraîner des ruptures de confidentialité (fuite de données à caractère personnel) nécessitant une notification à la CNIL pour violation de données.

De nombreuses publications peuvent guider vos équipes informatiques dans la **détection et la correction de ces vulnérabilités** qu'il est essentiel **d'engager au plus tôt** sur l'ensemble du périmètre de votre système d'information. Ceci pour vos propres composants ou pour des composants achetés à des tiers y compris en mode service (SAAS/CLOUD).

Les liens sont :

- Site de référence ANSSI CERT- FR:

  https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

- Alerte reprise par le CERT santé dans le lien suivant :
  https://www.cyberveille-sante.gouv.fr/alertes/2882-vulnerabilite-critique-dans-apache-log4j-activement-exploitee-mise-jour-le-13122021
  Le lien ci-dessus décline : les risques, les vecteurs d'infection, les systèmes affectés, les mesures réactives, etc.

Etienne Champion
Secrétaire général des ministères sociaux

Signé

Jean-François Parguet
FSSI des ministères sociaux

Signé