Une vulnérabilité critique dans Log4j a été découverte

NOUS RECOMMANDONS À NOS UTILISATEURS DE METTRE À JOUR LEURS PRODUITS TOUCHÉS DÈS QUE POSSIBLE

Vendredi dernier, une vulnérabilité critique a été détectée dans le projet Apache log4j (CVE-2021-44228). Pour les logiciels utilisant la bibliothèque, le simple fait de journaliser une chaîne de caractères d'un format spécifique peut conduire à l'exécution de code à distance. Log4j 2.15 corrigeant ce problème, nous recommandons à nos utilisateurs de mettre à jour leurs produits touchés dès que possible.

Nous avons procédé à un examen approfondi et sommes en mesure de confirmer que les produits et services de Devolutions ne sont pas **visés** par cette vulnérabilité.

Détails et mesure d'atténuation des risques

LunaSec propose une excellente description de la façon dont cette vulnérabilité peut être exploitée si vous êtes curieux de connaître les détails. En résumé, il suffit de journaliser une chaîne dans un format spécifique pour qu'une application vulnérable puisse télécharger et exécuter du code arbitraire à partir d'un serveur LDAP distant. Comme log4j est la bibliothèque de journalisation standard des applications Java, un très grand nombre de systèmes et de services sont concernés.

Les projets utilisant log4j doivent être mis à jour vers la version 2.15 dès que possible. Le projet log4j fournit également d'autres mesures d'atténuation.

Nous recommandons également à nos utilisateurs de mettre à jour leurs systèmes qui sont touchés par cette vulnérabilité. Le Nationaal Cyber Security Centrum a publié une liste avec l'état des vulnérabilités pour les produits des principaux fournisseurs.