Oracle publie un correctif d'urgence pour WebLogic Server

Oracle a publié dimanche une mise à jour de sécurité hors cycle pour Oracle WebLogic Server. Le nouveau patch corrige une vulnérabilité critique (CVE-2020-14750) d'exécution de code à distance (RCE – remote code execution).

Oracle WebLogic Server est une plateforme unifiée de développement, déploiement et exécution d'applications d'entreprise, dont Java, sur site et dans le cloud.

Les versions affectées du serveur d'applications sont les suivantes : versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 et 14.1.1.0.0.

Un premier correctif tronqué

Le mois dernier, dans le cadre de son « Critical Patch Update » d'octobre 2020, Oracle a mis à disposition des utilisateurs de WebLogic Server un premier correctif lié à la faille CVE-2020-14882. Celle-ci peut être exploitée par un attaquant, sans authentification.

« Des codes d'attaque ont été publiés le lendemain et des rapports publiés en source ouverte font état de campagne d'attaques », a relevé le CERT-FR.

> *Mise à jour de l'alerte CERT-FR*
>
> *CERTFR-2020-ALE-022 : [MàJ] Vulnérabilité dans Oracle Weblogic (02 novembre 2020). Un nouveau correctif a été publié par l'éditeur.https://t.co/mmPtvhirHJ*
>
> *— CERT-FR (@CERT_FR) November 2, 2020*

Dans ce contexte, Oracle a émis une alerte de sécurité le 1er novembre pour signaler que ce premier correctif ne corrige pas complétement la vulnérabilité d'exécution de code arbitraire à distance. Le nouveau patch est conçu pour combler les manquements.

L'éditeur logiciel de Redwood City (Californie) a prévenu :

« En raison de la gravité de cette vulnérabilité et de la publication sur divers sites de codes pour l'exploiter, Oracle recommande vivement aux clients d'appliquer les mises à jour fournies par cette alerte de sécurité dès que possible. »

À défaut, il est recommandé de désactiver temporairement la console WebLogic.

(crédit photo de une © Shutterstock)