

Oracle corrige ses serveurs d'application dans l'urgence

Une nouvelle vulnérabilité frappe les produits Oracle. Les plates-formes Oracle Application Server et Oracle Fusion Middleware, basées sur le logiciel de serveur HTTP open source Apache 2.0 ou 2.2, sont au centre d'une faille de sécurité, qui a forcé la firme de Larry Ellison [à réagir](#). Oracle incite donc à mettre à jour ses serveurs d'applications en question. [La vulnérabilité Apache a, elle, été corrigée fin août](#).

Sont précisément concernés par cette mise à jour critique d'Oracle, les produits suivant :Oracle Fusion Middleware 11g Release 1 (versions 11.1.1.3.0, 11.1.1.4.0 et 11.1.1.5.0); Oracle Application Server 10g Release 3 (10.1.3.5.0), et Oracle Application Server 10g Release 2 (10.1.2.3.0). La faille peut être exploitée pour lancer une attaque de type déni de service (DoS ou Denial of Service). Et cela sans même qu'il soit besoin de préciser un nom d'utilisateur et un mot de passe.

Une gravité 5 sur l'échelle d'Oracle, 7,8 sur celle du gouvernement

Un script Perl tel que Apache Killer peut l'exploiter. C'est un 'Header' spécifique (du nom de 'Range') qui sert au script pour submerger le serveur avec un très grand nombre de fichiers. Celui-ci peine alors à gérer ce flux d'informations simultanément et le crash s'avère inévitable.

Si Oracle reconnaît la gravité de la faille, sur l'échelle d'évaluation des vulnérabilités ('CVSS' pour 'Common Vulnerability Scoring System'), elle lui donne une note de « seulement » 5 sur 10. *« Un DoS sur l'OS complet est impossible sur aucune des plates-formes supportées par Oracle, et par conséquence, Oracle a noté la vulnérabilité avec un score de 5,0 indiquant un DoS complet du serveur HTTP Oracle mais pas de son système d'exploitation », se justifie l'éditeur.*

Cela va à l'encontre de la note de 7,8 sur 10 que le gouvernement américain avait donné à cette faille, rappelle [l'Espresso.fr](#). Quoi qu'il en soit, la menace est suffisamment pesante pour qu'il convienne d'effectuer promptement cette mise à jour majeure. D'ailleurs, Oracle lui-même la considère comme très sérieuse puisque l'éditeur est sorti de son cycle de mise à jour habituel (le prochain étant prévu pour le 18 octobre) pour proposer son correctif.