Le serveur web Apache victime d'une vulnérabilité critique « zero day »

La société de sécurité Qualys a émis, la semaine dernière, une alerte sur une faille de sécurité qui affecte le serveur open source Apache HTTP. Application, pour mémoire, utilisée pour la majorité des serveurs web de la planète (près de 65 % selon Netcarft). La vulnérabilité est liée à la configuration du Reverse Proxy *« qui pourrait permettre l'accès au système depuis Internet »*, selon **Prutha Parikh**, de Qualys, qui a découvert le problème. Le Reverse Proxy est notamment utilisé pour le *caching* ou l'équilibre de charges (*load balancing*).

Il s'agit dans les faits d'un problème précédemment rencontré (CVE-2011-3368) et auquel Apache avait proposé un correctif (à travers la version Apache 2.2.21 du serveur). Mais apparemment, la vulnérabilité persiste si les règles du reverse proxy ne sont pas configurées correctement. Une adresse web volontairement mal formée permettrait ainsi de contourner les règles de sécurité et accéder aux arcanes du système.

Si la fondation Apache a publiquement révélé l'existence du bug, aucun correctif n'est pour l'heure proposé. La seule solution pour se protéger des tentatives d'attaques pour l'heure est de configurer correctement le Reverse Proxy notamment en définissant correctement les instructions « RewriteRule » et « ProxyPassMatch ».

crédit photo © faberfoto Fotolia.com