Une faille dans Java et Python fragilise les firewalls

Deux chercheurs ont découvert une faiblesse de sécurité dans Java et Python. Le premier, Alexander Klink, a trouvé une faille dans la façon dont Java gère les liens FTP. Plus exactement, il ne vérifie par la syntaxe des noms d'utilisateurs dans le protocole FTP. Dans un blog, il précise que le bug est probablement ancien.

Dans le détail, il indique « *RFC 959 spécifie qu'un nom d'utilisateur peut se composer d'une séquence comprenant n'importe lequel des 128 caractères ASCII sauf <CR> (retour chariot) et <LF> (saut à la ligne). Devinez ce que les spécialistes de JRE ont oublié ? De vérifier la présence de <CR> ou <LF>. Cela signifie que si nous mettons % 0D% 0A n'importe où dans l'URL (ou dans la partie mot de passe), nous pouvons finaliser la commande USER (ou PASS) et injecter une nouvelle commande dans la session FTP* ». Un pirate peut ainsi forcer l'envoi de mails via le gestionnaire d'URL FTP Java. Cette lacune est appelée « injection de protocole ». Elle n'est pas nouvelle. Le laboratoire russe OnSec les avait mis en exergue en 2014 sans avoir reçu d'échos dans la communauté.

Python et les pare-feu n'y échappent pas

Un autre chercheur, Timothy Morgan de Blindspot Security, rajoute sa touche en découvrant que ce bug dans Java et aussi présent dans certaines librairies Python (urllib et urllib2). Mais à la différence d'Alexander Klink, le spécialiste s'est servi de cette faiblesse pour contourner des équipements de sécurité comme les pare-feux. L'injection de protocole peut être exploitée pour démarrer une connexion FTP classique utilisée par la plupart des pare-feu. L'attaque est relativement facile assure le spécialiste en réussissant à convaincre les utilisateurs à accéder à des applications malveillantes Java ou Python installées sur un serveur.

Pour l'exploit sur Java, les utilisateurs doivent avoir installés Java en local, même si les applest Java sont désactivées dans le navigateur, avertit le chercheur. En effet, le client Java va lire en priorité les fichiers JNLP (Java Networlk Launch Protocol) avant de faire autre chose. Il suffit alors pour l'attaquant de placer une URL FTP malveillante dans un fichier JNLP.

L'avantage de cette technique est qu'elle ouvre la voie à de multiples scénarios : attaques de type homme du milieu (MiTM) ou Server-Side Request Forgery (SSRF). Timothy Morgan a testé cette faille avec succès sur des firewalls de Cisco et Palo Alto Networks. Il précise que d'autres constructeurs pourraient être vulnérables via leurs OS Linux embarqués. Morgan a signalé les bugs à Oracle (en novembre 2016) et Python (janvier 2016), mais les deux organisations n'ont toujours pas corrigé ce bug. En attendant d'hypothétiques correctifs, le chercheur donne sur son blog des conseils pour se protéger de cette vulnérabilité.

A lire aussi :

Oracle creuse la tombe du plugin Java pour les navigateurs

Wikipédia : Java plus consulté que Steve Jobs ou Google

crédit photo © shutterstock