Une attaque Shellshock cible les serveurs de mail

La faille ShellShock, résidant dans Bash, l'interpréteur de lignes de commande le plus utilisé sur les systèmes Unix et Linux, a beau dater de plus d'un mois, elle demeure un vecteur d'attaques de choix. Selon une **alerte** **publiée par le SANS Internet Storm Center** (programme d'une société privée de formation américaine surveillant l'activité malicieuse sur le Net), des assaillants exploitent la vulnérabilité afin de tenter de faire exécuter des scripts Perl sur des machines compromises. En ciblant en particulier les passerelles SMTP (protocole de transfert des courriels vers les serveurs de messagerie). Objectif : **faire grossir un réseau d'ordinateurs zombies (botnet)** commandé par IRC.

« *L'attaque exploite Shellshock comme principal vecteur d'attaque via les champs subject, body, to et from* » des e-mails, précise Binary Defense System dans un billet de blog. « *Nous recommandons aux organisations de* ***s'assurer que tout système utilisant Bash a été patché*** *ou doit l'être immédiatement* », ajoute cette société spécialisée dans la sécurité managée, la réponse aux incidents ou l'analyse de menaces. Selon l'Internet Storm Center, les organisations qui ont fait état d'une attaque de ce type sont toutes des hébergeurs Web.

Des exploits Shellshock ont été utilisés dès les premières heures suivant la découverte de la vulnérabilité. Très souvent pour rechercher des systèmes vulnérables ou pour les faire entrer dans un botnet exploité dans le cadre d'attaques par déni de service (DDoS).
Concrètement, la faille ShellShock permet de modifier des variables d'environnement et d'**exécuter du code à distance** par le biais de scripts Apache CGI, des options DHCP et OpenSSH.

A lire aussi :
5 questions sur la faille Shell Shock visant Bash

Crédit photo : © drx – Fotolia.com