Faille Shell Shock : Les RSSI oscillent entre pragmatisme et attentisme

Point de concentration des responsables de la sécurité des systèmes d'information, les **Assises de la sécurité 2014** présentaient donc l'occasion de poser la question sur l'impact de la faille Shell Shock dans Bash au sein de leur entreprise. Une chose est sûre, la médiatisation du Bashbug n'a pas enflammé les allées du salon. Interrogé sur cette vulnérabilité que d'aucun prédise comme plus impactante que Heartbleed, Guillaume Poupard, directeur général de l'ANSSI a **minimisé le problème**. « *Il s'agit d'une faille parmi tant d'autres et nous avons alerté sur notre site les différents bulletins de sécurité, ainsi que les recommandations sur les correctifs à mettre en place.* »

Pour les RSSI, les réactions ont été variées sur cette faille avec une discrétion assumée. La plupart des responsables sécurité rencontrés **ont été informés très tôt** de cette vulnérabilité par les éditeurs de sécurité. Ils saluent cette rapidité dans la diffusion, tout comme la mise à disposition de correctifs même incomplets pour les distributions Linux. Certains avouent avoir attendu un peu pour s'y intéresser. « *Il y a eu du buzz à partir de jeudi (date de la publication de la faille) et puis les médias nationaux se sont emparés du sujet, nous nous sommes donc intéressés au sujet.* »

Une situation contrastée sur les réponses

Les responsables font donc confiance à leurs partenaires sécurité pour mettre à jour les signatures des menaces dans les IPS (systèmes de prévention d'intrusion) et leur faire remonter les informations sur les évènements de sécurité. Pour beaucoup, cette première barrière a été suffisante et ils n'ont **pas constaté une hausse sensible des attaques**. Il est vrai que sur les radars des spécialistes de la sécurité, les Etats-Unis représentent aujourd'hui le plus grand foyer d'attaques basées sur le bug de Bash. Si l'information est passée en mode alerte, les RSSI restent encore dans le flou sur la définition de la menace. Ainsi, peu d'entre eux savent qu'il existe non pas un mais **6 bulletins de sécurité liés à bash**.

Face à cette faille, la réponse à la menaces reste très variée en fonction de l'architecture IT de l'entreprise. *« Nous n'avons pas de systèmes Linux ou Unix, nous sommes plutôt dans des environnements Windows* », explique un responsable sécurité dans le domaine du transport énergétique. Pour certains, la question se règle différemment. « *Nos systèmes n'utilisent pas Bash mais d'autres solutions pour interpréter les commandes.* » D'autres évoquent des risques minimes. « *Nos systèmes ne sont pas sur Internet, il est donc plus difficile d'intégrer un script CGI malveillant sans intervention extérieure.* »

Cette bulle de protection reste néanmoins ténue notamment avec des systèmes de plus en plus connectés et selon **Cesar Cerrudo**, directeur technique de la société IOActive Labs, « *un attaquant peut utiliser Shellshock pour exécuter à distance tout type de code sur le système, la faille peut être exploitée pour* ***créer un ver qui va s'auto-répliquer****. Ce dernier utiliserait un seul système compromis pour attaquer d'autres systèmes et ainsi de suite, se propageant rapidement sur le réseau et contaminant des centaines de milliers de systèmes en peu de temps* ».

La phase audit est amorcée

D'autres sont plus pragmatiques et ont aussitôt commandé un audit de leurs systèmes. « *Nous disposons d'un parc comprenant des systèmes Unix et nous avons débuté un audit pour connaître notre exposition à la faille* », explique un responsable de la sécurité infrastructure d'un groupe du CAC 40. Une orientation confirmée par les éditeurs de solutions de sécurité. **Laurent Heslault**, directeur des stratégies de sécurité, précise : « *La vulnérabilité Shell Shock va permettre au moins une chose comme dans le cadre de Heartbleed, c'est de faire un inventaire des solutions et systèmes en entreprise* ».

Les grandes banques françaises ont joué la Grande Muette sur cette affaire. Aucun commentaire n'a été donné officiellement sur la faille Shell Shock. Mais les équipes sécurité ont été rapidement sollicitées pour faire une analyse des risques encourus.

Au final, les RSSI et DSI présents aux Assises de la sécurité à Monaco ont adopté une posture oscillant entre attentisme et pragmatisme. La faille, certes âgée de 22 ans, a été diffusée une semaine avant l'évènement et **les réponses dans les entreprises peuvent mettre un certain temps dans leur mise en œuvre**. Elle aura au moins eu le mérite d'observer les réactions faces aux menaces et de confirmer le lien de confiance avec les éditeurs de solutions de sécurité pour les aider à résoudre ce problème.

A lire aussi :

Apple corrige la faille Shell Shock pour Mac OS X sauf Yosemite
Faille Shell Shock : la riposte IT s'organise autour de Bash