Faille Shell Shock : la riposte IT s'organise autour de Bash

La fin de semaine et le week-end a été studieux pour les experts en sécurité qui se sont penchés sur la faille Shell Shock qui touche l'interpréteur de commande Bash. Cette vulnérabilité découverte par un français la semaine dernière, mais **vieille de 22 ans**, a semé la panique par son potentiel et par les premières attaques recensées sur différentes cibles, dont le ministère de la Défense américain et Akamai.

Distribution Linux et services Cloud

Touchant plusieurs systèmes allant des distributions Linux aux serveurs web, des objets connectés aux systèmes industriels, le monde de l'IT s'est organisé pour préparer la riposte face à cette menace. En première ligne, les distributions Linux qui ont rapidement corrigé cette faille. Cependant, **Red Hat** avait indiqué que son correctif n'était pas complet et a annoncé sur son blog la découverte d'autres exploits possible *via* la faille Shell Shock. L'éditeur a donc pris le temps du week-end pour publier des correctifs plus complets sur l'ensemble des vulnérabilités.

Du côté des fournisseurs de services web et Cloud en particulier, l'heure est aussi à la réparation rapide. **Google** a indiqué à nos confrères du *Wall Street Journal* avoir pris des mesures pour fixer le bug dans ses propres serveurs et les services Cloud proposés. Concernant App Engine, la firme de Mountain View recommande aux utilisateurs de mettre à jour les distributions Linux utilisées dans les instances créées. De même, **Amazon Web Services** a publié rapidement un bulletin de sécurité pour avertir ses clients de mettre à jour des images Linux ou AMI (un package d'image Linux pré-configurée) comprenant des versions vulnérables de Bash.

Apple a très tôt précisé que **la majorité des utilisateurs de Mac OS X** ne seront pas touchés par le Bash Bug. Mais, la firme a promis travailler sur un correctif pour rassurer complétement les experts en sécurité.

Cisco et Oracle sur le pont

Le matériel n'est pas exempt de cette course contre la montre pour remédier à cette faille. **Cisco** a audité une première salve de produits et a découvert 31 solutions vulnérables. Parmi eux, on retrouve des routeurs et des switches de la gamme Nexus, mais également des produits de sécurité (IPS, service d'identité, etc). Le constructeur annonce avoir mis à jour les logiciels et a créé une signature pour son IPS et les solutions Snort (issues de SourceFire) pour reconnaître et bloquer des attaques *via* la faille Shell Shock.

Oracle en pleine conférence OpenWorld à San Francisco ne pouvait faire impasse sur cette question. Le constructeur a indiqué qu'au moins **32 de ses solutions étaient vulnérables**. Il a rapidement proposé des correctifs pour les appliances Database, Exadata, Exalogic, Exlytics et bien évidemment les OS Oracle Linux (en version 4,5,6) et Solaris (8,9, 10, 11). L'éditeur dresse une liste

complémentaire de services et produits en cours d'analyse et devrait proposer prochainement des patchs sans donner de date précise.

Les NAS en mode rustine

Le monde de la sauvegarde n'est pas épargné notamment les NAS. **Synology et QNAP** sont montés au créneau en fin de semaine pour alerter leurs clients sur les menaces. QNAP a souligné dès vendredi que les utilisateurs de Turbo NAS seraient impactés et donnait des recommandations en l'absence de correctifs. Le constructeur vient de publier aujourd'hui une version corrigée de QTS et dresse la liste des produits concernés. Synology a fait le même constat en listant les produits touchés. Par contre, il n'a pas encore publié de correctifs.

La liste des mises à jour devrait s'allonger dans les prochaines heures et jours. Cette faille inquiète fortement les entreprises. Aux États-Unis, un groupe de régulateurs financiers qui prescrit des standards communs pour les établissements bancaires a exhorté ses membres à auditer et corriger le plus rapidement cette faille. Les avertissements vont se multiplier et les RSSI vont avoir du pain sur la planche ces prochaines semaines.

crédit photo@mathiasmeisenthal-shutterstock

A lire aussi :

5 questions sur la faille Shell Shock visant Bash