5 questions sur la faille Shell Shock visant Bash

A en croire les spécialistes de la sécurité, la **faille Shell Shock** est pire que la vulnérabilité Heartbleed qui avait touché la librairie de chiffrement Open Source, OpenSSL. En visant l'interpréteur de commande Bash dans les systèmes Linux ou certains OS, elle ouvre la boîte de Pandore des risques et des menaces. Nous avons posé 5 questions à des spécialistes de la sécurité informatique pour en savoir plus sur cette vulnérabilité.

1-Comment a été découvert Shell Shock ?

La faille a été découverte par un français, **Stéphane Chazelas**, qui travaille actuellement en Angleterre pour le fournisseur de CDN Akamai. Spécialiste du monde Linux/Unix et des télécoms comme l'indique sa page personnelle, il a trouvé un bug dans Bash (Bourne-Again shell) qui est un interpréteur de lignes de commande via des scripts. Il existe depuis plus d'une vingtaine d'années années (1993) et est devenu l'interprète standard de plusieurs systèmes Unix et distributions Linux, mais aussi des systèmes d'exploitation comme Mac OS X, Android et de manière plus limitée Windows avec le projet Cygwin.

Dans un entretien accordé à FairFax Media, Stéphane Chazelas précise que la découverte s'est déroulée il y a deux semaines. Il a aussitôt alerté Chet Ramey, en charge du support du code source Bash. En parallèle, il a aussi averti des fournisseurs d'infrastructures web et des éditeurs de distribution Linux comme Debian, Red Hat, Ubuntu, SuSE et Mandriva. Le problème est que « *cette découverte a été débattue rapidement sur des forums réduisant ainsi le temps pour trouver une réponse de la part de l'ensemble des acteurs* », explique **Thierry Karsenty**, directeur technique Europe chez CheckPoint.

Concrètement, la faille Shell Shock 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 en s'appuyant sur Bash. Shell Shock est souvent comparée à Heartbleed. **Loïc Guezo**, directeur Europe du Sud chez Trend Micro, écarte néanmoins cette analogie. « *Shell Shock n'est pas une faille traditionnelle. Dans le cas de Heartbleed, la vulnérabilité concernait la collecte de données, dans le cas de Bash, il s'agit d'une prise de contrôle d'un système ou d'un équipement.* »

2-Qui est touché par la faille Shell Shock ?

Le responsable de Trend Micro souligne que dans cette affaire, « *la prévalence de Bash dans le monde Linux est immense. On peut estimer à* ***500 millions le nombre d'équipements qui fonctionnent avec Bash*** ». Une analyse corroborée par **Guillaume Lovet**, expert en cybercriminalité chez Fortinet pour qui « *51% des serveurs web dans le monde tournent sous Apache (et donc probablement Linux, les deux allant généralement ensemble); or sur la plupart des distributions Linux, la version de Bash est vulnérable* ».

Les fournisseurs de services web sont donc aux premières loges sur l'exposition à la faille. Pour Thierry Karsenty, **les fournisseurs de Cloud** se sont emparés rapidement du problème comme le montre la décision d'AWS de rebooter pendant le week-end son Cloud pour corriger Xen. Une décision qui pourrait être dictée par l'annonce de Shell Shock.

« *De nombreuses appliances et systèmes embarqués reposent sur cet interpréteur de lignes de commande* », ajoute **Arnaud Soullié**, auditeur senior en sécurité pour Solucom. Les vecteurs d'attaques semblent illimités, allant **des hotspots WiFi** pouvant être compromis à travers le protocole DHCP ou **les objets connectés** qui embarquent des environnements Linux, jusqu'aux **systèmes industriels**. Même **la monnaie virtuelle Bitcoin** pourrait être impactée par cette faille. « *Beaucoup de systèmes pour miner les bitcoins repose sur des appliances qui utilisent Bash. Par ailleurs, le Bitcoin Core qui est au centre de la synchronisation entre les différents groupes s'appuie également sur l'interpréteur de commande* », constate Loïc Guézo.

Sur les systèmes d'exploitation, les experts en sécurité restent mesurés sur les conséquences de la faille. Apple a minimisé son impact sur les utilisateurs de Mac OS X. La firme de Cupertino a indiqué que « *l**a grande majorité des utilisateurs Mac ne risquent rien*** », cela ne l'empêche pas de prévoir un correctif dans les prochains jours pour les clients concernés. Pour les distributions Linux, l'ensemble des éditeurs ont annoncé des mises à jour avec parfois quelques ratés comme Red Hat qui est revenu sur son premier correctif.

3-Est-ce que la faille est utilisée ?

La réponse est clairement oui. Loïc Guézo confirme « *une activité notamment avec la découverte d'un malware nommé **Bash Lite** qui utilise clairement la vulnérabilité pour s'installer sur des machines. Nous avons aussi identifié le serveur Commande et Contrôle qui s'oriente vers **des attaques en DDoS*** ». Les autres éditeurs de sécurité constatent également une effervescence dans le cyberespace.

« *Il s'agit d'**une arme magique*** », s'exclame Thierry Karsenty et d'ajouter : « *Tout le monde est en train de regarder ce qu'il peut faire avec cette arme qui est une véritable porte ouverte dans les systèmes d'informations y compris pour les gouvernements. On constate une forte progression de l'activité de scan de ports pour savoir quel matériel est vulnérable, un serveur, un routeur, des terminaux Android*, etc. » A tel point que la faille n'est plus appelée Shell Shock, mais **Bashdoor** en référence aux portes dérobées existantes. Pour Thierry Karsenty, il s'agit d'un effet de bord à la publication rapide de la découverte de la faille. « *Nous sommes maintenant dans l'urgence et la pression pour corriger cette faille.* »

4-Comment savoir si on est vulnérable ?

Guillaume Lovet de Fortinet propose de réaliser un test echo. « *Il suffit de lancer un terminal et de taper la commande suivante, en respectant les espaces : env var='() { :;};echo Vulnerable' /bin/bash -c /bin/true. Si le résultat affiche « Vulnerable », alors le système est… Vulnérable !* »

Cette technique peut apparaître simple, mais rapportée à la surface d'attaque elle peut se révéler compliquée à systématiser. Notamment en entreprise. « *Cela va prendre du temps pour faire*

l'inventaire de ce qu'il faut corriger », prévient Thierry Karsenty. « *On découvrira certainement des vieux systèmes qui fonctionnent toujours et qui utilisent Bash, mais qui n'auront pas nécessairement à faire l'objet d'un correctif.* »

Une inquiétude pour le monde de l'entreprise partagée par Loïc Guézo. « *Il existe beaucoup de piles dans le système d'information aujourd'hui et Bash s'inscrit dans l'outil de production, il est donc très difficile de travailler dans l'urgence.* » Trend Micro propose néanmoins pour les utilisateurs des outils pour savoir si les équipements et les PC sont vulnérables à ShellShock.

5-Quels sont les remèdes ?

En premier lieu, il est impératif de **mettre à jour les équipements ou les différents OS** avec les correctifs émis par les éditeurs. La plupart d'entre eux ont été réactifs pour proposer des patchs, mais il ne s'agit pas du remède idéal. « *Le correctif de sécurité publié est incomplet, et des preuves de concept (PoC) permettant d'exploiter la vulnérabilité après application du correctif existent* », précise Arnaud Soullié de Solucom.

Il n'en demeure pas moins que pour l'instant la mise à jour est la première solution préconisée. En complément, les fournisseurs de solutions de sécurité recommandent d'**utiliser les infrastructures de sécurité existantes** pour trouver des parades et limiter les dégâts. « *Il est intéressant d'avoir des systèmes de protection (notamment, dans ce cas, IPS), qui vont protéger les systèmes vulnérables pendant que les patchs sont en test* », soumet Guillaume Lovet. **L'analyse contextuelle** devra être sollicitée de plus en plus en analysant « *les volumétries, les comportements, les flux* » de certaines applications et des systèmes, prévient Thierry Karsenty.

Au final, les premiers remèdes sont déjà disponibles, mais il faudra attendre les prochains jours ou semaines pour avoir des réponses complètes pour se protéger ou réduire l'impact des attaques via la faille Shell Shock.

Crédit Photo@isaak55-Shutterstock

A lire aussi :

Faille Heartbleed : la check-list pour s'en sortir

5 mois après : le bilan de la faille Heartbleed