Faille Shellshock dans Bash : pourquoi la tempête est loin d'être terminée

« *Nous ne savons toujours pas combien de systèmes sont vulnérables au bogue Shellshock, mais cela se chiffre vraisemblablement en millions.* » Dans une tribune publiée cette semaine sur la MIT Technology Review, **Cesar Cerrudo**, le directeur technique de la firme de sécurité IOActive Labs, résume assez bien le **désarroi et l'inquiétude** de la communauté des spécialistes en sécurité. Une semaine après la divulgation de cette faille affectant **l'interpréteur de commande Bash** (Bourne again shell) présent dans de nombreux systèmes **Linux mais aussi Unix, BSD, z/OS (l'OS des mainframes IBM) ou Mac OS**, la réponse à la menace reste insuffisante.

Or le risque est, lui, bien supérieur à Heartbleed, autre faille qui a défrayé la chronique en avril dernier. Tandis que cette dernière permettait à des attaquants de récupérer des données en mémoire (dont, potentiellement, des clefs de cryptage ou des mots de passe), les possibilités offertes par Shellshock sont bien plus larges, puisque cette vulnérabilité permet de prendre le contrôle d'un système, même sans login et mot de passe adéquats. Exploitée avec succès, **Shellshock donne tout simplement à un assaillant la capacité à exécuter les mêmes commandes qu'un administrateur**. Et cette exploitation est simple et ne requiert pas de compétences pointues, ajoute Cesar Cerrudo. De nombreux kits d'exploitation, scripts ou démo seraient déjà disponibles.

« *Comme 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* », imagine le directeur technique dans ce qui ressemble à un scénario catastrophe.

Linux embarqué : la présence insidieuse de Bash

De facto, la société américaine spécialisée en sécurité FireEye fait état d'un trafic important relatif à l'exploitation de Shellshock, trafic émanant probablement pour partie de Russie selon elle. Objectifs selon FireEye : des attaques DDoS (par déni de service), l'injection de malwares, l'exfiltration de données, la création de backdoors… Selon une autre société spécialisée, Incapsula, qui parle de 1 800 domaines attaqués sur son réseau et de 725 attaques à l'heure, les assaillants utilisent **des scanners pour repérer les systèmes vulnérables**.

Un constat d'autant plus inquiétant qu'il n'existe pas à ce jour de liste exhaustive des systèmes concernés par le bogue. Si le chercheur en sécurité **Rob Fuller** maintient sur GitHub une liste des systèmes pour lesquels des exploits semblent réalisables (la plupart concernant des serveurs Web faisant tourner des services CGI ou SSH), celle-ci est loin d'être exhaustive.

Par exemple, **Cisco** a d'ores et déjà identifié plus de 70 produits concernés, issus de familles les plus diverses ! Bien plus que le nombre de produits qui ne sont pas exposés. Et le géant des réseaux a encore une liste de près de 170 produits à vérifier ! **Oracle** a, de son côté, publié des

patch pour 9 produits (dont ses machines Exadata, Exalogic, Exalytics ou SuperCluster ou encore 4 versions de Solaris) et indiqué que 42 autres références sont probablement affectées. Chez **Juniper**, si la liste est moins longue, la plate-forme de management Junos Space est concernée, dans toutes ses versions. De son côté, **VMware** a recensé une quarantaine de produits impactés pour lesquels le spécialiste de la virtualisation a ou est en train de développer des patches. Majoritairement des appliances virtuelles Linux, même si l'hyperviseur ESX (versions 4.0 et 4.1) est lui aussi touché. Si de grands fournisseurs en sont encore à **évaluer l'étendue des dégâts**, on imagine ce qu'il en est de concepteurs plus exotiques de webcam IP, de points d'accès Wifi ou de box Internet embarquant un Linux… Qui représentent pourtant un risque bien réel. FireEye a ainsi détecté une attaque Shellshock visant les **systèmes NAS du constructeur taïwanais QNAP**.

Une faille ? Non, six… pour l'instant

Si la situation apparaît confuse, c'est surtout que Bash n'est pas affecté par une faille mais par une **flopée de vulnérabilités**, découvertes au fil des jours. Résumons : identifiée sous le nom de code CVE-2014-6271, la faille Shellshock a rapidement été patchée par les principaux distributeurs de Linux. Sauf qu'un ingénieur de Google a rapidement découvert que ce correctif pouvait être contourné, donnant naissance à une autre Common Vulnerability and Exposure (CVE), la CVE-2014-7169, qui elle aussi permet d'exécuter des commandes à distance. Deuxième patch émanant des principaux éditeurs de distributions.

Quatre jours plus tard, le 28 septembre, rebelote : deux ingénieurs de Google découvrent deux autres failles (CVE-2014-7186 et CVE-2014-7187). Certes moins sévères – elles ne permettraient pas l'exécution de code à distance, mais de mener par exemple des attaques par déni de service -, ces failles expliquent par exemple **le correctif incomplet publié par Apple**. Selon les chercheurs en sécurité de Rapid7, le patch de Cupertino ne comble pas CVE-2014-7186, elle aussi présente dans MacOS.

Et la liste ne s'arrête pas là. Coup sur coup, le 27 et le 30, Michal Zalewski (alias lcamtuf), autre employé de Google et découvreur de failles bien connu, lance **deux nouveaux pavés dans la mare**, alias CVE-2014-6277 et CVE-2014-6278. Deux vulnérabilités de Bash qui reçoivent le **score de criticité maxima**l, car elles permettent là encore l'exécution de code à distance. Si les détails techniques ne sont pas connus, les patches précédents des éditeurs de distribution seraient inopérants, selon un billet de blog d'lcamtuf. Ce dernier recommande l'installation d'un correctif créé par un ingénieur de Red Hat, Florian Weiner, et basé sur le filtrage des variables d'environnement. Une méthode radicale.

OpenVPN pris dans les filets

Si les deux dernières vulnérabilités ne semblent pas avoir été exploitées pour l'instant, le nombre de failles et la surface d'attaques que présente Bash sont évidemment des facteurs inquiétants. Car **les vecteurs sont nombreux pour accéder à l'interpréteur Bash** des systèmes ciblés : serveurs HTTP exploitant une interface CGI (Common Gateway Interface) ou FastCGI, clients DHCP, services SSH (Secure Shell) en particulier. Il faudra probablement **des semaines, voire des mois**, avant que les concepteurs de services, appliances ou appareils divers parviennent à mettre à jour leurs

systèmes. Sans oublier quelques mauvaises surprises, comme la vulnérabilité d'OpenVPN, package logiciel Open Source permettant de créer des réseaux privés virtuels… lui-même embarqué dans nombre d'autres systèmes.

Signalons que FireEye explique que **les sondes IPS et d'autres équipements de surveillance réseau** sont très efficaces pour détecter les exploits Shellshock. En effet, la séquence de code permettant d'activer la vulnérabilité est très spécifique et facile à analyser. Le risque de faux positifs serait donc limité. Une consolation. En attendant mieux.

crédit photo © drx – Fotolia.com

A lire aussi :

5 questions sur la faille Shell Shock visant Bash

Faille ShellShock : la riposte IT s'organise autour de Bash