Vulnérabilité Bash : les attaques Shellshock reviennent en force

Les vieilles failles de sécurité faciles à exploiter ont la vie dure. Il y a toujours quelque part un système qui n'a pas été corrigé. La faille Shellshock en est un vivant exemple. Deux ans après la découverte de cette vulnérabilité zero day touchant l'interpréteur de commandes Bash, force est de constater que la brèche est loin d'être complètement bouchée. Selon IBM, l'orifice est même encore assez béant.

La division Managed Security Services (MSS) de Big Blue a pu le constater en analysant de récentes attaques. Rien qu'en août dernier, le service a comptabilisé pas moins de 7 500 événements liés à la faille Shellshok, pourtant corrigée depuis sa découverte (même si les premiers patchs se sont révélés incomplets). Et, pour le deuxième anniversaire de l'exploitation de cette vulnérabilité vieille de plus de 20 ans, septembre promet de belles performances également. *« Au 22, le mois de septembre a représenté plus de 26 % de l'activité totale [de Shellshok] enregistrée en 2016 »*, écrit Michelle Alvarez, experte en sécurité chez IBM MSS.

Près de 8 000 attaques Shellshock par mois

L'essentiel (70 %) des attaques venaient des Etats-Unis et d'Australie (18 %). Elles visaient des organisations installées en Amérique du Nord (pour 26 %), au Japon (18 %) en Inde (16 %) et au Brésil (11 %). Même si les attaques Shellshock ont sérieusement décliné à partir d'octobre 2015, la vulnérabilité référencée CVE-2014-6271 reste vivace. Sur l'ensemble de l'année 2016, IBM évalue le nombre d'attaques liées à la faille à 7 900 par mois en moyenne. Les premières à en faire les frais sont les entreprises du secteur IT (à hauteur de 46 %), y compris les opérateurs télécoms, suivies des services financiers (26 %), des industries de fabrication (16 %), de la santé (6 %) et du commerce (5 %).

Rappelons que GNU Bash est un outil largement utilisé par les administrateurs systèmes pour gérer les environnements Unix, Linux, Solaris ainsi que Mac OS X. Autant d'environnements informatiques déployés dans des environnements professionnels pointus où les mises à jour systèmes ne sont pas toujours triviales en raison de contraintes de production et du besoin de stabilité. Des contraintes dont profitent les cybercriminels, qui trouvent là des cibles facilement accessibles.

Lire également

Faille Shell Shock : Les RSSI oscillent entre pragmatisme et attentisme
Faille Shellshock dans Bash : pourquoi la tempête est loin d'être terminée
Comment Ikea a corrigé rapidement la faille Shellshock