Backdoor ou erreur de code dans les firewall de Juniper

On trouve parfois de drôle de choses dans le code des systèmes d'exploitation. Une équipe de Juniper vient d'en faire l'expérience en découvrant au sein de son OS ScreenOS des solutions de firewall et VPN, ce qu'elle appelle pudiquement un bout de *« code non autorisé »*. Dans un bulletin de sécurité (CVE-2015-7755) émis par Juniper, ce code « *pourrait donner à un attaquant averti l'accès aux produits NetScreen et la capacité de déchiffrer les connexions VPN* ».

L'équipementier a indiqué avoir créé un correctif qui est en phase de déploiement auprès des clients concernés. Juniper précise que c'est la gamme NetScreen (fonctionnant avec les versions 6.2.0r15 à 6.2.0r18 et 6.3.0r12 à 6.3.0r20 de ScreenOS) qui est concernée. Il se veut rassurant en précisant qu'après une première analyse, aucune attaque utilisant cette vulnérabilité n'a été détectée. Certes, mais « *le code non autorisé* » est présent dès la version 6.2.0r15 de ScreenOS qui a été publié… en 2008. Les potentiels attaquants ont donc disposé de 8 ans pour commettre leur méfait et retourner ensuite dans l'ombre.

Backdoor de la NSA ou erreur de développement ?

Les seules interrogations qui demeurent sont : comment et qui a placé ce « *code non autorisé* » dans le code source de ScreenOS ? S'agit-il d'une backdoor (porte dérobée) d'un Etat ou d'une agence gouvernementale comme la NSA ? Les documents dévoilés par Edward Snowden montrent que l'agence américaine a intégré des mouchards dans des équipements réseaux, notamment ceux de Cisco avant leur expédition. Un article de 2013 du Spiegel pointe un programme de la NSA baptisé FEEDTHROUGH visant les firewall de Juniper de la gamme Netscreen.

Bien sûr, il existe d'autres hypothèses pouvant la présence de ce code exogène : ce pourrait ainsi être l'œuvre d'un développeur malintentionné ou d'un hacker subtil. Avec des OS datant de près d'une dizaine d'année, il sera difficile de remonter au responsable. D'autant que Juniper ne dispose pas d'un système de contrôle de version (CVS)…

Non content d'avoir trouvé ce code étranger, Juniper en profite aussi pour corriger une autre vulnérabilité. La faille permet un accès distant non autorisé à un terminal via SSH ou Telnet. « *Cette attaque peut conduire à une compromission complète du système* », précise le bulletin de sécurité de l'équipementier.

A lire aussi :
Juniper Networks dissocie son OS Junos de ses équipements réseaux
Juniper Networks veut unifier le réseau de l'entreprise avec Unite