Juniper : une faille de sécurité permettait de surveiller le trafic VPN

	Une faille de sécurité permettait de surveiller le trafic VPN

La firme indique avoir découvert des portes dérobées dans ScreenOS, présent dans ses pare feux et services VPN. Par mesure de sécurité, Juniper a mis à jour son système d'exploitation.

Juniper indique qu'un morceau de code informatique non-autorisé était présent dans son système d'exploitation maison. Ce dernier est utilisé pour une partie de ses solutions de sécurité tels que les firewall et les services de VPN. La société a donc émis un bulletin de sécurité au sujet de ce code-espion.
Ce dernier aurait été initialement publié en 2008, de quoi laisser le temps aux éventuels attaquants d'utiliser cette porte dérobée pour utiliser des informations transitant par le biais de ces équipements. Un correctif est donc actuellement déployé par Juniper, en particulier pour les équipements de la gamme NetScreen.
Malgré ces mises à jour de sécurité, Juniper n'a pas identifié la provenance de ce code aux effets malfaisants. Si la thèse des services de renseignement n'est pas à exclure, il pourrait également s'agir de hackers ou même de développeurs présents en interne (voire des sous-traitants).

La porte dérobée doit en principe permettre à un attaquant d'accéder à distance en mode administration à un équipement sous ScreenOS. Quant à la seconde vulnérabilité mise au jour par Juniper, elle autorise un pirate à surveiller un trafic au sein d'un VPN.
Malgré l'ampleur du problème, la direction se veut rassurante. Elle précise : « pour le moment, aucun rapport n'indique que ces vulnérabilités ont été exploitées. Nous recommandons vivement aux clients de mettre à jour leurs systèmes et d'appliquer les versions corrigées sans délai ».

Réagissez à cet article

Source : *Juniper : une faille de sécurité permettait de surveiller le trafic VPN*