Cyber sÃ©curitÃ© : Palo Alto Networks protÃ¨ge de la faille #Heartbleed
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 17/4/2014 13:30:00

Palo Alto Networks, leader du marchÃ© de la sÃ©curitÃ© d'entreprise, garantit la protection contre la faille Heartbleed, littÃ©ralement Â« coeur qui saigne Â» (vulnÃ©rabilitÃ© CVE- 2014-0160) pour ses clients Entreprise.
Selon lâalerte US Cert (TA14 - 098A) documentÃ©e le 8 Avril 2014, cette vulnÃ©rabilitÃ© au niveau du protocole OpenSSL permettrait Ã un pirate distant dâatteindre les donnÃ©es sensibles, des informations et clÃ©s secrÃ¨tes d'authentification (ex : mot de passe, codes bancaires, donnÃ©es partagÃ©es avec le site) des utilisateurs via la mÃ©moire du serveur du site consultÃ©, en utilisant les extensions heartbeat du protocole.

Â« *Beaucoup de gens sont inquiets depuis l'alerte sur la faille de sÃ©curitÃ© Heartbleed. Pour ma part, je suis rassurÃ© car j'ai vu que nous Ã©tions dÃ©jÃ protÃ©gÃ©s via notre plate-forme de sÃ©curitÃ© Palo Alto Networks* Â», commente **Neal Moss**, Analyste SystÃ¨mes et RÃ©seau et infrastructure informatique chez BYU Hawaii.

Â« *L'ampleur du risque portÃ© par Heartbleed va bien au-delÃ des applications Web comme Yahoo!, Google et Facebook. Avoir de la visibilitÃ© et une bonne gestion des vulnÃ©rabilitÃ©s qui peuvent sâabattre sur une entreprise peut Ãªtre un dÃ©fi de taille.*

Parce que Palo Alto Networks dispose dâun vÃ©ritable temps dâavance pour protÃ©ger contre des failles telle que Heartbleed grÃ¢ce Ã sa plateforme de sÃ©curitÃ© de nouvelle gÃ©nÃ©ration, nous avons Ã©tÃ© en mesure de prÃ©venir le danger, dâagir pour nos clients et limiter l'exploitation de cette faille Â», tÃ©moigne **Raj Shah**, directeur de la cyber sÃ©curitÃ© chez Palo Alto Networks.

Pour ses clients, Palo Alto Networks fournit une protection unique contre l'exploitation de la faille Heartbleed, y compris :

ï· Une approche innovante dâidentification des menaces : Contrairement Ã d'autres produits de sÃ©curitÃ©, notre plate-forme dÃ©code nativement l'ensemble du trafic dÃ¨s la couche d'application, quel que soit le port et le protocole utilisÃ©, y compris les tunnels SSL/TLS.

Par consÃ©quent, Palo Alto Networks est en mesure de dÃ©composer le protocole SSL (dans ce cas) pour dÃ©tecter les anomalies, chose que ne font pas les dispositifs de sÃ©curitÃ© du rÃ©seau existant.

ï· Une protection automatisÃ©e contre les vulnÃ©rabilitÃ©s : Des mises Ã jour de contenus multiples sont automatiquement envoyÃ©es Ã nos clients depuis le 9 Avril 2014. Ces protections de vulnÃ©rabilitÃ© dÃ©tectent et bloquent immÃ©diatement toute tentative dâexploitation de la faille (mises Ã jour de contenus 429 et 430, qui comprennent les signatures IPS avec les IDs 36416, 36417, 36418. et 40 039).

ï· CaractÃ©ristiques et fonctionnalitÃ©s inhÃ©rentes au PAN-OS. Notre systÃ¨me d'exploitation de base (PAN- OS), nâest pas affectÃ© par la rÃ©fÃ©rence CVE-2014-0160 car il n'utilise pas la version vulnÃ©rable de la bibliothÃ¨que OpenSSL.

Pour les entreprises qui ne sont pas clients Palo Alto Networks et qui se prÃ©occupent de leur cyber-sÃ©curitÃ©, Palo Alto Networks recommande au minimum, la mise Ã jour des serveurs Web Ã la derniÃ¨re version Â« patchÃ©e Â» de OpenSSL disponible depuis le 7 Avril 2014 (l 1.0.1g), et un remplacement immÃ©diat des clÃ©s privÃ©es SSL aprÃ¨s la mise en place du patch.

En savoir plus sur la vulnÃ©rabilitÃ© Heartbleed

La vulnÃ©rabilitÃ© Heartbleed est associÃ©e Ã une faille critique dÃ©celÃ©e dans OpenSSL. Elle a Ã©tÃ© rÃ©cemment rÃ©vÃ©lÃ©e et affecte les serveurs exÃ©cutant OpenSSL version 1.0.1 Ã 1.0.1f soit " *plus de 17 % des serveurs Web SSL qui utilisent des certificats dÃ©livrÃ©s par les autoritÃ©s de certification de confiance.* " Au pire, la faille peut conduire Ã la compromission de la totalitÃ© du contenu placÃ©e sur n'importe quel serveur exÃ©cutant des versions affectÃ©es dâOpenSSL, y compris les services internes.

Pour plus dâinformation sur la vision et lâaction de Palo Alto Networks pour Ã©radiquer Heartbleed.

Â