VPN : Cisco alerte ses clients sur une grave vulnérabilité

Décidément, ce début d'année 2018 est secoué par des vulnérabilités graves affectant des composantes vitales des systèmes d'information.

Dernière faille majeure en date, celle annoncée hier par **Cisco** qui affecte la fonctionnalité WebVPN d'une série d'appliances : Firepower 2100 Series, Firepower 4110, Firepower ISA (Industrial Security Appliance) 3000 Series, ASA (Adaptive Security Appliance) 5500 Series, ASA 5000-X (pare-feu de nouvelle génération), ASA 1000V (Cloud Firewall) mais aussi l'appliance virtuelle ASAv, ainsi que son logiciel FTD 6.2.2 (Firepower Threat Defense).

Si l'alerte est si inquiétante, c'est que le bug découvert (CVE-2018-010) est affublé d'une sévérité maximale de niveau 10.

Il permet en effet à un attaquant d'envoyer des paquets XML (spécialement assemblés) pour entraîner le reboot du système affecté et même l'exécution à distance de codes malveillants.

En pratique, un attaquant peut aisément prendre le contrôle total de ces systèmes clés pour la sécurité du système d'information pour peu que la fonctionnalité WebVPN de ces logiciels et appliances Cisco ait été activée.

La vulnérabilité a été récemment découverte par Cedric Halbronn, chercheur en sécurité du NCC Group.

Cisco fournit des instructions à l'intention des administrateurs sur comment désactiver la fonctionnalité incriminée et les invite à migrer sur les dernières versions de ces logiciels afin de bénéficier des patchs déjà disponibles.

Le constructeur assure n'avoir pas connaissance de la moindre exploitation de cette faille jusqu'à aujourd'hui par des cybercriminels.

(Crédit photo : Pare-feu Cisco FirePOWER 2100)