Cisco lance une alerte sur une faille de sécurité dans IOS

Selon l'agence*NetworkWorld*, le système d'exploitation IOS pour *« Internetworking Operator System »* utilisé dans les routeurs, les points d'accès WiFI et les commutateurs de Cisco, peut être piraté par un hacker utilisant à distance la fonctionnalité FTP du système d'exploitation.

Même si cette fonctionnalité FTP (File Transfert Protocol) est désactivée par défaut, la vulnérabilité est bien réelle et dangereuse.

Le FTP de l'IOS est utilisé pour uploader des données vers les routeurs et les commutateurs à distance. Toutefois selon Cisco, des hackers peuvent exploiter cette vulnérabilité dans le serveur FTP pour accéder au système de fichiers d'un équipement utilisant l'IOS. Il peut par exemple profiter d'une telle intrusion pour modifier des fichiers ou la configuration d'un routeur…

*« En utilisant cette faille, des utilisateurs non autorisés peuvent modifier la configuration d'un équipement, et la façon dont ce dernier démarre. Le fichier de démarrage contient des informations que ces pirates peuvent réutiliser pour obtenir des droits privilégiés généralement réservés aux administrateurs du réseau… »*indique Cisco.

Par conséquent, le groupe offre à ses clients un patch refermant cette porte dérobée. En plus de ce correctif, Cisco conseille à ses usagers de fermer la fonctionnalité FTP de IOS. La commande à saisir pour fermer le serveur est la suivante : « no ftp-server enable ».)

Les versions 11.3, 12.0, 12.1, 12.2, 12.3 et 12.4 de IOS sont touchées par cette faille. L'IOS XR n'est pas vulnérable.

Rappelons qu'en mai 2004, 800 Mo de IOS versions 12.3 et 12.3t, avaient été illégalement copiés et publiés sur un site Web où tout un chacun aurait pu le télécharger pendant quelques jours.

Selon le *New York Times*, après un an d'enquête de la part des autorités américaines, il apparaît que le vol à été à l'origine de nombreuses intrusions dans certains autres systèmes informatiques comme celui de la NASA, de plusieurs organismes militaires américains et de laboratoires de recherche.