Cisco panse les switches vulnérables aux zero days de la CIA

Début mars 2017, Wikileaks dévoilait des techniques de piratage employées par la CIA pour s'attaquer à nombre de produits d'industriels afin de pénétrer les systèmes. Techniques qui s'appuient la plupart du temps sur des failles de sécurité zero day. Parmi les victimes potentielles, figuraient plus de 300 modèles de switches Cisco affectés d'une vulnérabilité de niveau critique (CVE-2017-3881). Vulnérabilité aujourd'hui corrigée.

Dans une alerte mise à jour lundi 8 mai dernier, le constructeur met à disposition une version corrigée de ses OS réseau IOS et IOS XE qui comblent la faille en question. Celle-ci affectait le Cluster Management Protocol (CMP), qui utilise le protocole Telnet pour lancer des commandes sur un réseau interne. La vulnérabilité *« pourrait permettre à un attaquant distant non authentifié de recharger un périphérique affecté ou d'exécuter un code à distance avec des privilèges élevés »*, rappelle Cisco dans son alerte.

Mise à jour incontournable

Le spécialiste réseau souligne qu'il *« n'y a pas de solution de contournement »* à cette vulnérabilité. Sauf à configurer le système pour exclure l'usage de Telnet (et s'en priver), la mise à jour est donc… incontournable.

Cisco n'avait pas été le seul acteur majeur touché par des failles exploitées par les agents de la CIA. Selon le site de Julian Assange, Microsoft, Apple et Samsung, parmi d'autres, figurent aussi dans la liste des entreprises dont les produits étaient ciblés par l'agence américaine de renseignements. Le lanceur d'alerte avait néanmoins annoncé que les documents publiés en mars (baptisés Vault 7), et issus d'un Wiki interne à la CIA, ne dévoilaient pas précisément le code pour mener des attaques. Wikileaks entendait travailler avec les acteurs de l'industrie informatique pour leur laisser le temps de corriger leurs vulnérabilités avant d'éventuelles publications plus précises sur ces techniques d'attaques. Cisco, qui avait été l'un des premiers acteurs à en alerter ses clients, ne donne aucune précision sur cette éventuelle collaboration, ni sur des attaques potentiellement en cours. Mais entend aujourd'hui mettre à l'abri ses consommateurs des *exploits* de la CIA.

Lire également
Wikileaks : les outils de hacking de la CIA seront « désarmés » avant publication
10 questions pour comprendre l'affaire Shadow Brokers
Cisco aurait développé un nouvel OS réseau

crédit photo © Inara Prusakova – shutterstock