Cisco : le protocole CDP encore sujet à des failles

En dépit des nombreux correctifs dont il a déjà fait l'objet, CDP reste vulnérable.

Les découvertes d'Armis l'illustrent.
L'entreprise californienne – à l'origine d'une plate-forme de sécurité d'entreprise orientée IoT – a trouvé cinq failles dans diverses implémentations de ce protocole de découverte réseau implémenté sur l'essentiel des équipements Cisco.

Ce dernier, averti fin août 2019, vient de publier des patchs.

Quatre des failles en question ouvrent la porte à l'exécution de code à distance. Elles sont créditées d'un score de 8,8/10 sur l'échelle CVSS.

- CVE-2020-3119
  Elle touche le système d'exploitation NX-OS, embarqué dans des *switchs*.
  Le problème réside au niveau du traitement des paquets CDP destinés à gérer l'alimentation électrique des périphériques sur Ethernet (PoE).
  La vulnérabilité se déclenche par l'envoi d'instructions qui contiennent davantage de niveaux de gestion d'énergie que le *switch* n'en attend. Elle occasionne un débordement de pile.
- CVE-2020-3118
  Elle affecte le système d'exploitation pour IOS-XR, embarqué dans des routeurs.
  Le souci se trouve dans le traitement de champs (identifiant de port, d'appareil…) que contiennent les paquets CDP.
  La vulnérabilité s'enclenche plus précisément en ajoutant certains caractères dans les paramètres transmis à la fonction sprintf. Elle entraîne également un débordement de pile.

Téléphones : le point faible ?

- CVE-2020-3111
  Celle-ci concerne des dizaines de modèles de téléphones IP Cisco. Elle est liée à la fonction de traitement des identifiants de ports.
  Le fait que les téléphones acceptent les paquets CDP transmis en unicast et en broadcast donne davantage de liberté pour exploiter la faille. Pas besoin, en l'occurrence, d'envoyer le paquet malveillant depuis le *switch* auquel est connecté le téléphone. Et il est possible d'attaquer en une fois tous les téléphones résidant sur un même LAN.
- CVE-2020-3110
  Les caméras IP série 8000 en sont victimes. Le traitement des identifiants de ports en est à nouveau la source, mais l'effet est différent : dépassement de tas. Ces risques peuvent être limités par le recours à l'ASLR (distribution aléatoire de l'espace d'adressage), mais le *daemon* CDP des caméras série 8000 ne l'implémente pas.

La cinquième faille (CVE-2020-3120) touche à la fois IOS-XR et NX-OS. Elle se déclenche en faisant allouer au démon CDP de gros blocs de mémoire, de sorte qu'il plante et fasse redémarrer routeurs et *switchs* (déni de service).

La vulnérabilité des *switchs* est particulièrement problématique. Elle peut permettre de contourner les mesures de segmentation de réseau potentiellement mises en place pour mieux protéger les appareils.

*Photo d'illustration © Prayitno / Thank you for (12 millions +) view*via*Visual Hunt / CC BY*