Attaque sophistiquée sur les routeurs Cisco IOS

Cisco alerte sur les risques d'attaques de ses routeurs. *« Cisco a observé un nombre limité de cas où les attaquants, après avoir obtenu un accès physique ou via les droits d'administration à un périphérique IOS, ont remplacé le ROMMON par une image ROMMON malveillante »*, prévient l'équipementier dans sa notification publiée le 11 août.

Une menace persistante

Rappelons que IOS est le système d'exploitation qui accompagne la plupart des routeurs et switches de l'américain. Le ROMMON, ou ROM Monitor, est le **logiciel de bas niveau** qui se met en route au démarrage de la machine et lance IOS après les configurations et vérifications de base du matériel. Autrement dit, l'équivalent pour un équipement réseau du Bios ou de l'UEFI pour un PC. Remplacer le ROMMON officiel dans un routeur par une image corrompue de celui-ci revient à installer une menace qui persistera même après la réinitialisation du matériel et constituera, potentiellement, une porte d'entrée permanente sur le réseau.

Cisco se veut néanmoins rassurant. *« Aucune vulnérabilité produit n'est exploitable dans cette attaque et les attaquants doivent disposer des droits d'administration valides ou d'un accès physique au système pour parvenir à leurs fins. »* Il n'en reste pas moins que le *flashage* du ROMMON est parfaitement documenté et à la portée de tout administrateur réseau.

Protéger les identifiants d'administration

Pour se protéger, au-delà de la surveillance physique des équipements, les entreprises devront donc s'assurer que les droits d'administration restent bien gardés. Pour s'attaquer aux routeurs, les intrus tenteront probablement d'acquérir les identifiants de connexion des administrateurs par tous les moyens possibles, leur imagination dans ce domaine étant souvent fertile.

Toujours est-il que Cisco ne détaille pas, dans son alerte, comment certains de ses équipements ont été compromis. Le constructeur se contente d'évoquer *« des attaques de plus en plus complexes »*. Mais la mise à jour du firmware ne nécessite visiblement aucune signature numérique ou un système de chiffrement du code qui protègerait l'appareil des attaques de ce type. L'entreprise invite les administrateurs à consulter sa documentation, publique et récemment mise à jour, pour intégrer les informations propres aux attaques ROMMON et aux autres menaces affectant ses produits IOS.

Lire également
Une faille SSH béante sur les appliances réseau Cisco
Recrudescence d'attaques DDoS depuis de «vieux» routeurs

3 à 6 mois pour détecter une attaque dans la Finance et le Retail

crédit photo © Inara Prusakova – shutterstock