Cisco corrige des bugs sur ses appliances de sécurité et son VPN

Le géant des réseaux Cisco est suffisamment présent dans les entreprises pour que l'on applique rapidement ses correctifs.

Cisco AnyConnect Secure Mobility Client

Produit professionnel d'accès à distance et VPN – connexion VPN SSL ou IPsec d'appareils exécutant un Cisco iOS vers les appliances Cisco 5500 ASA -, parfois déployé pour protéger la connexion entre un smartphone de type iPhone et le réseau de l'entreprise, AnyConnect Secure Mobility Client fait l'objet quatre vulnérabilités qui affectent les composants de téléchargement basés sur le web.

Elles permettent à un site mafieux de se camoufler derrière un site légitime et d'inciter le visiteur à instancier le composant vulnérable. Deux vulnérabilités permettent à l'attaquant d'exécuter un code malicieux, les deux autres dégradent le VPN vers une ancienne version. Sont concernées les plateformes Windows, Mac OS X et Linux.

Appliances Cisco ASA

Une faille permettrait à un attaquant distant non identifié de forcer les appliances ASA (Adaptive Security Appliances) de Cisco – ASA 5500 Series Adaptive Security Appliances et Cisco Catalyst 6500 Series ASA Services Module à redémarrer via une attaque par déni de service.

La plateforme de gestion ACE (Application Control Engine) fait également l'objet d'une vulnérabilité overlap IP qui pourrait permettre à un administrateur non repéré d'exécuter une instance virtuelle non souhaitée.

Dans tous les cas, la mise à jour devra être réalisée rapidement.