Failles dans Cisco IOS

Identifiées par Cisco, les deux failles de sécurité sont qualifiées de risque « élevé » par le site de veille FrSIRT. Leur exploitation par un attaquant distant pourrait lui permettre un accès aux ressources réseau du système impacté.

Selon FrSIRT, la première faille est la conséquence d'une erreur présente dans la fontion « XAUTH » du serveur « Easy VPN » qui, dans certains cas, ne manipule pas correctement les paquets reçus (port 500/udp). Son exploitation permet de contourner l'authentification Xauth et obtenir un accès aux ressources réseau. La seconde vulnérabilité est causée par une erreur présente dans la procédure d'authentification et d'assignation des profils ISAKMP. Son exploitation permet de contourner les restrictions sécuritaires. Les versions impactées de Cisco IOS sont les v12.2.x et les v12.3.x. Cisco donne le détail de ces failles et des solutions possibles à cette adresse.