Un nouveau déni de service sur Cisco IOS

Encore une faille chez Cisco. L'exploitation de la vulnérabilité est en plus triviale. Il suffit d'établir une connexion TCP (3-way handshake) sur le service Telnet (port 23) ou bien sur les services de Telnet inversé (ports 2001 a 2999, 3001 a 3099, 6001 a 6999, ou encore 7001 a 7099) puis de forger et envoyer un paquet malformé pour mettre en péril toute tentative de connexion ultérieure.

Une fois l'attaque effectuée, l'ensemble des services gérés par le terminal virtuel (VTY) tels que Telnet, Telnet inversé, SSH, RSH et dans certains cas HTTP deviennent inaccessibles. Les sessions déjà établies avec les services en question restent en revanche maintenues. L'attaque nécessitant une connexion TCP complète, les tentatives de « Spoofing » s'avèrent difficiles? Toutes les versions de l'Internetwork Operating System de Cisco sont affectées. Il est recommandé de combler cette vulnérabilité au plus vite. Cisco prévoit de fournir un correctif de sécurité dans les prochains jours et conseille de suivre certaines recommandations pour neutraliser temporairement la vulnérabilité.
Norman Girard pour Vulnerabilite.com