Cisco corrige une faille vieille de 3 ans dans Telnet

La vulnérabilité CVE-2011-4862 n'a pas battu la faille Shell Shock avec ses 22 ans d'ancienneté, mais elle commence à dater. De 3 ans pour être exact, car elle a été **découverte par le projet FreeBSD en 2011**. Cette faille touche Telnet, un protocole de type client-serveur s'appuyant sur TCP. Il est très présent dans les équipements réseaux.

Or le directeur de l'International Business Schools IT, Glafkos Charalambous, s'est aperçu que **Cisco n'avait toujours pas corrigé cette vulnérabilité**. Un problème non négligeable quand on sait que cette faille avait été intégrée il y a encore quelques temps dans des modules de Metasploit, le célèbre couteau-suisse des assaillants. Le chercheur a relevé ce bug **dans le logiciel AsyncOS** qui fonctionne sur plusieurs appliances de sécurité de la firme américaine (web, e-mail et gestion de contenu).

L'équipementier informé a aussitôt mis en garde ses clients des risques encourus (exécution de code arbitraire et élévations de privilèges notamment) si le protocole Telnet est activé sur ces appliances. Dans son avis, il explique que « *la vulnérabilité est due à des contrôles insuffisants lors du traitement des clés de chiffrement de Telnet* ». Dans le classement de niveau de compromission de Cisco, **cette faille atteint le maximum avec un score de 10** en raison de sa facilité d'exploitation et de l'importance de son impact.

A lire aussi :
Sécurité : Cisco invite ses clients à verrouiller WebEx
Cisco ASA 5500X FirePower, des firewall NextGen orientés menaces

crédit photo : tadamichi / shutterstock