Cisco corrige les serveurs de temps de ses offres réseau

Le géant des réseaux **Cisco** élimine les failles de sécurité de ses équipements et logiciels.

La firme corrige tout d'abord le **serveur de temps** intégré à nombre de ses produits. Une série de failles dans le serveur **ntpd** (Network Time Protocol daemon) permet aux pirates d'opérer des attaques par déni de service sur les produits Cisco, voire de changer l'heure qu'ils affichent.

11 bulletins de sécurité permettent de corriger de multiples failles, **jugées non critiques**, dans le Network Time Protocol. Ceci fait suite à la découverte de 12 failles le 19 janvier par le NTP Consortium. Des vulnérabilités qui touchent pratiquement toutes les offres Cisco. **72 sont citées** dans le bulletin de sécurité de la société. Ces problèmes ont maintenant été corrigés.

Des failles non corrigées

Une autre faille de gravité moyenne a été détectée dans **Cisco Unity Connection**. Des attaques de type XSS (*cross-site scripting*) peuvent être menées à l'encontre de l'interface web de gestion de cette offre. La firme communique sur ce souci, mais ne propose pas à ce jour de correctif. Voilà qui est original.

Le projet **OpenSSL** a récemment détecté deux failles dans sa pile SSL/TLS. Cisco estime que la gravité de ces vulnérabilités **reste élevée**. La société n'a toutefois pas encore pu déterminer lesquels de ses produits sont concernés par ces failles. À suivre.

À lire aussi :
Lenovo corrige deux failles de sécurité dans son outil de mise à jour
37 failles de sécurité corrigées dans Google Chrome 48
Adobe corrige 77 failles dans Flash !

Crédit photo : © World Economic Forum / Severin Nowacki