Depuis son origine, TCP/IP recèle une faille réelle

L'

US CERT Coordination Center, un organisme officiel américain, a révélé l'existence d'une faille dans le protocole de communication TCP (*Transmission Control Protocol*), un protocole critique présent au c?ur de l'Internet et de nombreux réseaux. Cette faille, présente dans TCP/IP depuis sa création et involontairement reproduite dans toutes ses implémentations, permettrait à un hacker de fermer prématurément une session TCP en engageant une attaque par déni de service. La faille peut aussi troubler des communications entre routeurs sur l'Internet en interrompant des sessions BGP (*Border Gateway Protocol*), car ces dernières très répandues utilisent TCP. C'est un chercheur en sécurité, Paul Watson, qui a décrit la faille dans un document nommé « *Slipping in the Window : TCP Reset Attacks*« . La principale surprise provient de la connaissance de ce type de faille par les experts en réseaux, depuis plus de 20 ans? Le standard TCP alloue une adresse 32 bits unique lorsqu'il établie une connexion, les suivantes s'enchaînent selon une séquence de nombres supérieurs théoriquement pré établie. Pourtant, il suffit à un hacker d'insérer une valeur 32 bits supérieure pour qu'elle soit acceptée comme une valeur exacte ! Avec l'évolution de l'internet et du volume des connexions, les acteurs du Net, et en particulier les fournisseurs d'accès, ont graduellement augmenté la taille de la fenêtre en autorisant des séquences de nombres avec une marge d'erreur, ce qui rend possible, voire facile, une attaque par déni de service. Les fabricants d'équipement réseaux devraient très rapidement corriger leurs produits, avant la fin de la semaine sans doute, en particulier ceux qui disposent de code BGP, très vulnérable aux attaques. Cisco vient d'ailleurs de mettre en ligne une mise à jour de sécurité. L'impact de la faille devrait donc être limitée, voire marginale.