CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-07(07)

Tunnellisation partagée pour les appareils distants

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-07(07) — Tunnellisation partagée pour les appareils distants (PaF-)

Énoncés :

Prévenir la tunnellisation partagée pour les dispositifs distants qui se connectent à des systèmes organisationnels à moins que le tunnel partagé soit fourni de façon sécurisée au moyen de [Affectation : mesures de protection définies par l'organisation].

Responsable : Aucun

Discussion :

La tunnellisation partagée est un processus qui consiste à permettre à une utilisatrice, un utilisateur ou un dispositif distant d'établir une connexion non distante à un système et de communiquer simultanément par l'entremise d'une autre connexion à une ressource située dans un réseau interne. Cette méthode d'accès réseau permet à une utilisatrice ou un utilisateur d'accéder à des dispositifs distants et, simultanément, d'accéder à des réseaux non contrôlés. La tunnellisation partagée peut s'avérer désirable par les utilisatrices et utilisateurs distants qui veulent communiquer avec les ressources du système local, notamment les imprimantes et les serveurs de fichiers. La tunnellisation partagée pourrait toutefois donner libre cours aux connexions externes non autorisées, rendant ainsi le système plus vulnérable aux attaques et aux exfiltrations d'information organisationnelle. On peut prévenir la tunnellisation partagée en désactivant les paramètres de configuration qui permettent une telle capacité dans des dispositifs distants et en empêchant ces paramètres de configuration d'être configurés par les utilisatrices et utilisateurs. La prévention peut également être réalisée par la détection de la tunnellisation partagée (ou des paramètres de configuration qui permettent la tunnellisation partagée) dans le dispositif distant, ainsi que par l'interdiction des connexions lorsque le dispositif distant utilise la tunnellisation partagée. Un RPV peut être utilisé pour fournir un tunnel partagé de manière sécurisée. Un RPV fourni de manière sécurisée comprend le verrouillage de la connectivité à des environnements exclusifs, gérés et nommés ou à un ensemble particulier d'adresses préapprouvées, sans l'intervention d'une utilisatrice ou un utilisateur.