

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du protocole PPTP sous Windows 2000 et Windows XP

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-239>

Gestion du document

Référence	CERTA-2002-AVI-239
Titre	Vulnérabilité du protocole PPTP sous Windows 2000 et Windows XP
Date de la première version	31 octobre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité Microsoft MS02-063
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de service.

2 Systèmes affectés

Microsoft Windows 2000 et Windows XP.

3 Résumé

Une vulnérabilité dans le traitement des données du protocole PPTP permet à un utilisateur mal intentionné de provoquer un déni de service à distance.

4 Description

PPTP (Point-to-Point Tunneling Protocol) est un protocole de type client-serveur permettant d'encapsuler des trames PPP dans des paquets IP. Il a été défini dans la RFC 2637 (cf. Documentation), et sert à la mise en place de

réseaux privés virtuels (VPN).

Ce protocole est natif dans les systèmes Microsoft Windows 2000 et Windows XP.

On le retrouve également comme composant optionnel dans les systèmes Windows NT 4.0, Windows 98, Windows 98 SE et Windows ME, mais l'implantation du protocole sur ces systèmes ne présente pas de vulnérabilité.

Le protocole PPTP définit une connexion de contrôle entre le client et le serveur (port 1723/tcp par défaut). Une vulnérabilité dans le traitement des données de cette connexion permet à un utilisateur mal intentionné, par le biais de paquets PPTP malicieusement construits, de provoquer un déni de service.

Cette vulnérabilité est exploitable à distance.

5 Solution

Appliquer le correctif publié par Microsoft (cf. section Documentation).

6 Documentation

Avis de sécurité Microsoft MS02-063 :

<http://www.microsoft.com/technet/security/bulletin/ms02-063.asp>

PPTP - RFC 2637 :

<http://www.ietf.org/rfc/rfc2637.txt>

Gestion détaillée du document

31 octobre 2002 version initiale.