

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Windows NT 4 dans le protocole PPTP

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-2001-AVI-018>

Gestion du document

Référence	CERTA-2001-AVI-018
Titre	Vulnérabilité sous Windows NT 4 dans le protocole PPTP
Date de la première version	14 février 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft (MS01-009)
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 NT 4.0 Server ;
- Microsoft Windows NT 4.0 Server, Entreprise Edition ;
- Microsoft Windows NT 4.0 Server, Terminal Server Edition.

3 Résumé

Un utilisateur mal intentionné peut créer un déni de service sur un serveur NT 4.0 en envoyant des paquets PPTP astucieusement formés.

4 Description

Le protocole PPTP (Point to Point Tunneling Protocol) permet d'effectuer le transfert d'informations de manière chiffrée. Une vulnérabilité découverte dans ce protocole rend possible la surcharge du système par le biais de paquets PPTP spécifiques. Il est alors nécessaire de redémarrer le serveur.

Nota : Aucune connexion PPTP valide, de l'utilisateur, n'est nécessaire pour exploiter cette vulnérabilité.

5 Solution

Appliquer le correctif (version US) disponible sur le site Microsoft :
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=27836>

Le correctif pour Windows NT 4.0 Server Terminal Server Edition n'est pas disponible actuellement.

6 Documentation

Bulletin de sécurité Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS01-009.asp>

Faq Microsoft :
<http://www.microsoft.com/technet/security/bulletin/fq01-009.asp>

Gestion détaillée du document

14 février 2001 version initiale.