

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans HyperTerminal de Microsoft

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-2004-AVI-394>

Gestion du document

Référence	CERTA-2004-AVI-394
Titre	Vulnérabilité dans HyperTerminal de Microsoft
Date de la première version	15 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-043
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

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

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 3 & Service Pack 4 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-bit Edition ;
- Microsoft Windows XP Service Pack 1 & Service Pack 2 ;
- Microsoft Windows XP 64-bit Edition Service Pack 1 & Version 2003.

3 Résumé

Une vulnérabilité présente dans l'HyperTerminal de Microsoft permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

L'application HyperTerminal présente une vulnérabilité de type dépassement de mémoire tampon, qui permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, au moyen d'une adresse réticulaire Telnet (URL) malicieusement constituée, dans la mesure où la victime décide d'ouvrir le lien malicieusement constitué avec l'application HyperTerminal.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS04-043 :
<http://www.microsoft.com/technet/security/bulletin/MS04-043.mspx>
- Référence CVS CAN-2004-0568 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0568>

Gestion détaillée du document

15 décembre 2004 version initiale.