Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 6 octobre 2005
N° CERTA-2005-AVI-214

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du client Telnet Microsoft

Gestion du document

Référence	CERTA-2005-AVI-214
Titre	Vulnérabilité du client Telnet Microsoft
Date de la première version	15 juin 2005
Date de la dernière version	6 octobre 2005
Source(s)	Bulletin de sécurité Microsoft MS05-033 du 14 juin 2005
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 avec Service Pack 1 ;
- Microsoft Windows Server 2003 pour Itanium et Microsoft Windows Server 2003 avec Service Pack 1 pour Itanium ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows Services pour UNIX versions 2.2, 3.0 et 3.5 sur plate-forme Microsoft Windows 2000 ;

3 Résumé

Une vulnérabilité dans le client Telnet de Microsoft permet à un utilisateur mal intentionné d'avoir accès à des informations sensibles sur le système vulnérable.

4 Description

Le client Telnet permet d'émuler un terminal à distance.
Une vulnérabilité dans la gestion de la commande `NEW-ENVIRON` permet à un utilisateur mal intentionné, via un serveur Telnet malicieux, d'avoir accès à des informations sensibles sur le système vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS05-033 du 14 juin 2005 :
  http://www.microsoft.com/technet/security/bulletin/MS05-033.mspx
- Bulletin de sécurité iDEFENSE 06.14.05 du 14 juin 2005 :
  http://www.idefense.com/application/poi/display?id=260&type=vulnerabilities
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1205

Gestion détaillée du document

15 juin 2005 version initiale.
6 octobre 2005 correction orthographique.