Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2004
N° CERTA-2004-AVI-341

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'interpréteur de commandes Windows

Gestion du document

Référence	CERTA-2004-AVI-341
Titre	Multiples vulnérabilités dans l'interpréteur de commandes Windows
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-037
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows NT Server 4.0 Service Pack 6 ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6a ;
- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP and Microsoft Windows XP service Pack 2 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition ;
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE) et Microsoft Windows Millenium Edition.

3 Résumé

Plusieurs vulnérabilités présentes dans l'interpréteur de commandes de Microsoft Windows permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités référencées sous les deux numéros CVE suivants sont présentes dans le système d'exploitation Microsoft Windows :

- CAN-2004-0214 : l'interpréteur de commandes de Microsoft Windows présente une vulnérabilité dans la méthode de démarrage d'un programme. Elle permet à un utilisateur à distance et mal intentionné, d'exécuter du code arbitraire à distance sur le système vulnérable, au moyen d'un site web malicieusement construit.
- CAN-2004-0572 : l'application `Program Group Converter` qui permet de convertir les groupes de programme des versions antérieures de Windows, présente une vulnérabilité lors la manipulation d'une requête. Un utilisateur mal intentionné peut exploiter cette vulnérabilité au moyen d'une requête malicieusement construite, dissimulée dans un lien HTML, pour exécuter un code arbitraire à distance.

Dans ces deux cas, l'utilisateur mal intentionné obtiendra les mêmes privilèges que ceux de la victime.

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 MS04-037 du 12 octobre 2004 :
  http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx
- Référence CVE CAN-2004-0214 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0214
- Référence CVE CAN-2004-0572 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0572

Gestion détaillée du document

13 octobre 2004 version initiale.