



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 octobre 2003
N° CERTA-2003-AVI-170

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les contrôles ListBox et ComboBox

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-2003-AVI-170>

Gestion du document

Référence	CERTA-2003-AVI-170
Titre	Vulnérabilité dans les contrôles ListBox et ComboBox
Date de la première version	16 octobre 2003
Date de la dernière version	–
Source(s)	Bulletin #MS03-045 de Microsoft
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

Elévation de privilèges.

2 Systèmes affectés

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

3 Résumé

Une fonction de la bibliothèque `User32.dll` présente une vulnérabilité de type débordement de mémoire. Cette fonction est utilisée par les contrôles `ListBox` et `ControlBox`.

4 Description

Les messages Windows permettent aux processus interactifs de réagir aux événements utilisateur ou de communiquer avec les autres processus interactifs.

L'une des fonctions de la bibliothèque `User32.dll` qui permet de fournir la liste des options d'accès aux utilisateurs ne valide pas correctement certains de ses paramètres pour les messages Windows qui lui sont envoyés. L'envoi d'un message malicieusement formé à un processus interactif peut faire exécuter aux contrôles `ListBox` et `ComboBox` du code arbitraire.

Un utilisateur mal intentionné peut utiliser cette vulnérabilité présente dans toutes les applications mettant en œuvre ces contrôles afin d'élever ses privilèges.

5 Solution

Appliquer le correctif suivant la version de Microsoft Windows concernée (cf. Documentation).

6 Documentation

- Bulletin de sécurité #MS03-045 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS03-045.asp>
- Référence CVE CAN-2003-0659 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0659>

Gestion détaillée du document

16 octobre 2003 version initiale.