

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le pilote de fonction connexe 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-2008-AVI-507>

Gestion du document

Référence	CERTA-2008-AVI-507
Titre	Vulnérabilité dans le pilote de fonction connexe de Microsoft
Date de la première version	15 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-066 du 14 octobre 2008
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 ;
- exécution de code arbitraire.

2 Systèmes affectés

- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows XP Professional x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 pour Itanium ;
- Microsoft Windows Server 2003 Service Pack 2 pour Itanium.

3 Résumé

Une vulnérabilité dans le pilote de fonction connexe de `Microsoft` permet à un utilisateur local malintentionné d'élever ses privilèges.

4 Description

Une vulnérabilité est présente dans le pilote de fonction connexe ou `Ancillary Function Driver` de `Microsoft`. Un manque de contrôle des données transmises du mode utilisateur au mode noyau permet à un utilisateur local d'exécuter du code arbitraire avec des privilèges très élevés sur le système.

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 MS08-066` du 14 octobre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-066.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS08-066.mspx>
- Référence CVE `CVE-2008-3464` :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3464>

Gestion détaillée du document

15 octobre 2008 version initiale.