



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2010
N° CERTA-2010-AVI-073

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le sous-système MS-DOS de Microsoft Windows

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-2010-AVI-073>

Gestion du document

Référence	CERTA-2010-AVI-073
Titre	Vulnérabilité dans le sous-système MS-DOS de Microsoft Windows
Date de la première version	10 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-015 du 09 février 2010
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

Élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 et Windows XP Service Pack 3 ;
- Windows XP Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Windows Vista, Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Windows Vista Édition x64, Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 bits.

3 Résumé

Une vulnérabilité dans le sous-système MS-DOS de Microsoft Windows peut être exploitée par un utilisateur local malintentionné afin d'élever ses privilèges.

4 Description

Une vulnérabilité dans le sous-système MS-DOS (`ntvdm.exe`) et affectant potentiellement toutes les versions 32 bits de Microsoft Windows, permet à un utilisateur local d'élever ses privilèges au moyen d'un exécutable spécialement construit.

Le savoir-faire nécessaire pour exploiter cette vulnérabilité est d'ores et déjà disponible sur l'Internet.

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 MS10-015 du 09 février 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-015.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-015.msp>
- Référence CVE CVE-2010-0232 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0232>

Gestion détaillée du document

10 février 2010 version initiale.