



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-336

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2004-AVI-336>

Gestion du document

Référence	CERTA-2004-AVI-336
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-032
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 ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Server Terminal Server Edition Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 3 ;
- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP ;
- Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP édition 64 bits Service Pack 1 ;
- Microsoft Windows XP édition version 2003 ;
- Microsoft Windows Server édition 64 bits ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows 98, Windows 98 Seconde Edition, Windows 98 Millenium Edition.

3 Résumé

Plusieurs vulnérabilités présentes dans les logiciels Microsoft Windows permettent à un utilisateur mal intentionné de réaliser un déni de service, d'élever ses privilèges ou d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Quatre vulnérabilités référencées sous les quatre numéros CVE suivants sont présentes dans les systèmes d'exploitation Microsoft :

- CAN-2004-0207 : une vulnérabilité est présente dans les APIs (Application Programming Interface) Windows. Cette vulnérabilité permet à un utilisateur mal intentionné déjà connecté au système d'obtenir des privilèges élevés sur le système.
- CAN-2004-0208 : une vulnérabilité est présente dans le composant chargé du traitement des VDM (Virtual DOS Machine) de Microsoft Windows. Cette vulnérabilité permet à un utilisateur mal intentionné déjà connecté au système d'obtenir des privilèges élevés sur le système. Aucune des versions de Windows 98 n'est affectée par cette vulnérabilité.
- CAN-2004-0209 : un débordement de mémoire présent dans le traitement des images aux formats EMF (Enhanced Metafile) et WMF (Windows Metafile) permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système. Les versions de Microsoft Windows 98 et de Microsoft Windows NT 4.0 ne sont pas affectées par cette vulnérabilité.
- CAN-2004-0211 : une vulnérabilité est présente dans le noyau de Windows. Cette vulnérabilité permet à un utilisateur local mal intentionné de réaliser un déni de service sur le système vulnérable. Seules les versions de Windows Server 2003 sont affectées par cette vulnérabilité.

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 MS04-032 :
<http://www.microsoft.com/technet/security/bulletins/MS04-032.msp>
- Référence CVE CAN-2004-0207 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0207>
- Référence CVE CAN-2004-0208 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0208>
- Référence CVE CAN-2004-0209 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0209>
- Référence CVE CAN-2004-0211 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0211>

Gestion détaillée du document

13 octobre 2004 version initiale.