



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2004
N° CERTA-2004-AVI-238

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du composant POSIX 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-2004-AVI-238>

Gestion du document

Référence	CERTA-2004-AVI-238
Titre	Vulnérabilité du composant POSIX de Microsoft
Date de la première version	15 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-020
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 Terminal Server Edition 4.0 Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 2, Service Pack 3 et Service Pack 4 ;

3 Résumé

Une vulnérabilité dans le composant POSIX de Microsoft permet à un utilisateur local d'élever ses privilèges.

4 Description

Le composant POSIX (Portable Operating System Interface for UNIX) de Microsoft permet d'exécuter des applications UNIX POSIX. Cette émulation est incluse dans Microsoft Windows NT 4.0 et

Microsoft Windows 2000 (Microsoft Windows XP et Microsoft Windows Server 2003 ne contiennent pas l'émulation POSIX).

Une vulnérabilité de type débordement de tampon est présente dans le composant POSIX et permet à un utilisateur local mal intentionné d'élever ses privilèges.

5 Solution

Se référer au bulletin de sécurité de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS04-020 du 13 juillet 2004 :
<http://www.microsoft.com/technet/security/bulletin/ms04-020.msp>
- Référence CVE CAN-2004-0210 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0210>

Gestion détaillée du document

15 juillet 2004 version initiale.