



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 novembre 2003
N° CERTA-2003-AVI-102-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Windows 2000

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-102>

Gestion du document

Référence	CERTA-2003-AVI-102-001
Titre	Vulnérabilités dans Windows 2000
Date de la première version	04 juillet 2003
Date de la dernière version	13 novembre 2003
Source(s)	Base de connaissances Microsoft Advisory CORELABS Advisory SNS
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

La première vulnérabilité affecte :

- Windows 2000 Server avec Active Directory activé.

La seconde vulnérabilité affecte les versions suivantes :

- Microsoft Windows 2000 Advanced Server ;
- Microsoft Windows 2000 Datacenter Server ;
- Microsoft Windows 2000 Professional ;
- Microsoft Windows 2000 Server.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans certaines versions de Windows 2000. Elles permettent à un utilisateur mal intentionné d'effectuer un déni de service ou bien d'exécuter du code arbitraire à distance.

4 Description

- LDAP (Lightweight Data Access Protocol) est un protocole standardisé permettant à un client d'interroger un annuaire situé sur un ou plusieurs serveurs. C'est l'un des protocoles utilisés dans Windows 2000 pour accéder à Active Directory.

L'envoi d'une requête LDAP malicieusement construite vers un serveur de domaine Windows 2000 permet à un utilisateur mal intentionné d'effectuer un déni de service ou bien d'exécuter du code arbitraire à distance.

- La primitive système *ShellExecute* présente dans la bibliothèque *shell32.dll* permet d'ouvrir ou d'exécuter un fichier associé à une extension connue. Cette API est utilisée dans de nombreuses applications telles que les navigateurs, les messageries ou certains éditeurs de texte.

Un débordement de tampon présent dans cette API permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance ou bien d'effectuer un déni de service.

5 Solution

Appliquer le Service Pack 4 pour Windows 2000.

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp>

6 Documentation

- Base de connaissances Microsoft 319709 :
<http://support.microsoft.com/default.aspx?kbid=319709>
- Advisory CORELABS (CORE-2003-0305-03) :
<http://www.coresecurity.com/common/showdoc.php?idx=351&idxseccion=10>

Gestion détaillée du document

04 juillet 2003 version initiale.

13 novembre 2003 Références sources.