Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 janvier 2002
N° CERTA-2002-AVI-018

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mauvaise gestion de l'appartenance à un domaine lors de l'authentification par SID sous Windows NT/2000

Gestion du document

Référence	CERTA-2002-AVI-018
Titre	Mauvaise gestion de l'appartenance à un domaine lors de l'authentification par SID sous Windows
Date de la première version	31 janvier 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS02-001
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

- Contournement des règles de sécurité ;
- Augmentation des privilèges.

2 Systèmes affectés

Windows NT et Windows 2000.

3 Résumé

Il est possible d'obtenir les privilèges de l'administrateur d'un domaine Windows NT/2000 sur les ressources partagées de ce dernier.

4 Description

Les ressources partagées d'un domaine Windows peuvent être accessibles depuis un autre.

Lorsqu'un utilisateur d'un domaine Windows désire accèder à une ressource partagée présente dans un autre domaine, les informations le concernant sont passées au domaine destination sous la forme d'une liste de SID (*Security IDentifiers*). Ce sont ces informations qui détermineront si l'accès lui est autorisé.

Malheureusement, il est possible d'usurper les SID d'un autre utilisateur et d'obtenir ainsi ses privilèges sur le domaine distant.

Pour cela, il est nécessaire d'avoir les droits d'administration du domaine d'origine.

5 Solution

Appliquer le correctif de microsoft :

- Pour Windwos NT Enterprise Server :
  http://www.microsoft.com/ntserver/ntsdownloads/critical/q299444/
- Pour Windows 2000 Server :
  http://www.microsoft.com/windows2000/downloads/critical/q311401/

6 Documentation

Bulletin de sécurité Microsoft MS02-001 :
http://www.microsoft.com/technet/security/bulletin/MS02-001.sap

Gestion détaillée du document

31 janvier 2002 version initiale.