Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 février 2001
N° CERTA-2001-AVI-020

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le contrôleur de domaine de Windows 2000 Server

Gestion du document

Référence	CERTA-2001-AVI-020
Titre	Vulnérabilité dans le contrôleur de domaine de Windows 2000 Server
Date de la première version	21 février 2001
Date de la dernière version	–
Source(s)	Avis Microsoft MS01-011
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.

2 Systèmes affectés

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

3 Résumé

Un utilisateur malveillant peut, par le biais de requêtes malformées envoyées à une machine contrôleur de domaine Windows 2000, entraîner un déni de service sur cette machine.

4 Description

Un des services du contrôleur de domaine sous Windows 2000 ne gère pas convenablement les demandes de traitements. Au lieu de rejeter directement une requête invalide, ce service essaie d'en effectuer le traitement

pour finalement envoyer une réponse d'erreur. Un utilisateur envoyant un flot continu de requêtes judicieusement malformées peut entraîner une augmentation de la consommation des ressources de la machines cible, forçant celle-ci à ne traiter que des demandes invalides au détriment des demandes valables. Ceci empêche ainsi le contrôleur de domaine d'enregistrer de nouveaux utilisateurs sur le domaine et empêche l'accès à la liste d'adresses actives.

5 Solution

Correctif fourni pour Windows 2000 Server et Windows 2000 Advanced Server :
http://www.microsoft.com/Downsloads/Release.asp?ReleaseID=28064

Concernant Windows 2000 Datacenter Server, Microsoft préconise de prendre contact avec le revendeur de ce matériel.

6 Documentation

Bulletin et Faq Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-011.asp

Gestion détaillée du document

21 février 2001 version initiale.