

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Windows 2000 dans la politique de sécurité locale

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-2000-AVI-037>

Gestion du document

Référence	CERTA-2000-AVI-037
Titre	Vulnérabilité sous Windows 2000 dans la politique de sécurité locale
Date de la première version	29 août 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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 Professional ;
- Microsoft Windows 2000 Server ;
- Microsoft Windows 2000 Advanced Server.

3 Résumé

Une vulnérabilité permet à un utilisateur mal intentionné, en corrompant une machine locale, de l'empêcher de participer à un réseau. Si cette vulnérabilité est exploitée sur un contrôleur de domaine, toute l'architecture du réseau peut être perturbée.

4 Description

La politique de sécurité locale sous Windows 2000 est un ensemble d'informations qui encapsule tous les aspects de sécurité sur la machine locale. Elle définit les utilisateurs, les groupes, les droits et les permissions. Par conception les utilisateurs non privilégiés ne peuvent pas effectuer des changements dans cette configuration.

Cependant une vulnérabilité existe dans la politique de sécurité locale. Un poste de travail ou un serveur de domaine peut être corrompu par un utilisateur (même non authentifié au domaine) par le biais d'une commande RPC (Remote Procedure Call).

5 Solution

Appliquer le service Pack 1 pour windows 2000 (version US):
<http://www.microsoft.com/Download/Release.asp?ReleaseID=24019>

6 Documentation

Bulletin de sécurité Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS00-062.asp>

Faq Microsoft :
<http://www.microsoft.com/technet/security/bulletin/fq00-062.asp>

Gestion détaillée du document

29 août 2000 version initiale.