Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juillet 2001
N° CERTA-2001-AVI-080

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Service pour Unix 2.0

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-2001-AVI-080

Gestion du document

Référence	CERTA-2001-AVI-080
Titre	Vulnérabilité dans Microsoft Services pour Unix 2.0
Date de la première version	25 juillet 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-039
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 Services pour Unix, version 2.0

3 Résumé

Deux composants des services pour Unix 2.0 (NFS et Telnet) sont affectés par une vulnérabilité permettant à un utilisateur mal intentionné d'entraîner un déni de service sur la machine qui offre ces services.

4 Description

Les services pour Unix peuvent être installés sur Windows NT ou Windows 2000 afin de faciliter l'intégration des machines Windows dans les environnements Unix.

– Première vulnérabilité :
  Le système de fichiers de réseau NFS est un protocole, défini par la RFC1094, permettant l'accès distant aux fichiers partagés.
  Une vulnérabilité dans la mise en œuvre NFS sous SFU 2.0 (Services For Unix) permet à un utilisateur mal intentionné, par le biais de requêtes astucieusement composées, de provoquer une fuite de mémoire entraînant un épuisement des ressources de la machine cible. Cette vulnérabilité peut obliger l'administrateur à effectuer un redémarrage de la machine.
– Seconde vulnérabilité :
  Une vulnérabilité présente dans le service Telnet du SFU, entraîne également une fuite de mémoire pouvant conduire à un épuisement des ressources du système de la machine cible.
  Nota : Cette vulnérabilité n'affectait pas le serveur Telnet de Windows NT4 ou Windows 2000 mais uniquement de SFU.

5 Solution

Télécharger les correctifs sur le site Microsoft :

– Première vulnérabilité (NS) :
  – Windows NT 4 :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31600
  – Windows 2000 :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31592
– Seconde vulnérabilité (Telnet) :
  – Windows NT 4 :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31601
  – Windows 2000 :
    http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31595

6 Documentation

Bulletin Microsoft
http://www.microsoft.com/technet/security/bulletin/ms01-039.asp

Gestion détaillée du document

25 juillet 2001 version initiale.