

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans *Services for Unix 3.0* de Microsoft

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-2002-AVI-222>

Gestion du document

Référence	CERTA-2002-AVI-222
Titre	Multiples vulnérabilités dans <i>Services for Unix 3.0</i> de Microsoft
Date de la première version	03 octobre 2002
Date de la dernière version	–
Source(s)	
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

- Dénier de service ;
- exécution de code arbitraire.

2 Systèmes affectés

Services for Unix (SFU) 3.0 Interix SDK sur les systèmes d'exploitation suivants :

- Microsoft Windows NT4 ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP.

3 Résumé

Trois vulnérabilités ont été découvertes dans la bibliothèque Sun RPC dans les *Services for Unix 3.0* développés par Microsoft.

4 Description

Microsoft *Services for Unix* (SFU) est un ensemble de services permettant d'intégrer Windows dans un environnement Unix existant. L'application Interix SDK, incluse dans la version SFU 3.0, fournit un environnement Unix au-dessus d'un noyau Windows, et comprend un certain nombre de compilateurs, d'outils, de bibliothèques et d'interpréteurs. Trois vulnérabilités affectent la bibliothèque Sun RPC incluse dans Interix SDK.

Une première vulnérabilité, de type débordement de mémoire, permet à un utilisateur distant mal intentionné de former une requête particulière afin d'effectuer un déni de service sur le serveur ou d'exécuter du code arbitraire.

Une deuxième vulnérabilité, liée à une mauvaise vérification par le serveur de la taille des données envoyées par le client, permet à un utilisateur distant mal intentionné de bloquer le serveur et de provoquer ainsi un déni de service.

Une troisième vulnérabilité est due à une erreur d'implémentation RPC et permet à un utilisateur distant mal intentionné de former une requête particulière afin d'effectuer un déni de service sur le serveur.

5 Contournement provisoire

Le filtrage au niveau du pare-feu sur le port 111/TCP permet d'éviter l'exploitation de ces vulnérabilités par un utilisateur distant. Il est cependant conseillé d'appliquer le correctif.

6 Solution

Appliquer le correctif fourni par Microsoft :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43447>

7 Documentation

Bulletin de sécurité Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS02-057.asp>

Gestion détaillée du document

03 octobre 2002 version initiale.