Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 octobre 2001
N° CERTA-2001-AVI-133

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ufsrestore sous Solaris.

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-133

Gestion du document

Référence	CERTA-2001-AVI-133
Titre	Vulnérabilité de ufsrestore sous Solaris.
Date de la première version	29 octobre 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun
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

Augmentation des privilèges en local.

2 Systèmes affectés

SunOS 5.8, 5.7, 5.6, 5.5.1, 5.5 sur plate-forme Sparc et x86.

3 Résumé

Un utilisateur mal intentionné peut obtenir les privilèges de l'administrateur `root` en local grâce à l'utilisation de la commande ufsrestore.

4 Description

Ufsrestore est un utilitaire de restitution de sauvegarde à partir d'un fichier créé par la commande ufsdump.

Un utilisateur mal intentionné peut, par le biais d'un débordement de mémoire de la commande ufsrestore, obtenir les privilèges de l'administrateur système `root`.

Cette vulnérabilité n'est exploitable qu'en local avec un utilisateur authentifié sur la machine.

5 Solution

Télecharger le correctif Sun selon la version du système :

- SunOS 5.8 : 109091-04
- SunOS 5.8x86 : 109092-04
- SunOS 5.7 : 106793-07
- SunOS 5.7x86 : 106794-07
- SunOS 5.6 : 105722-06
- SunOS 5.6x86 : 105723-06
- SunOS 5.5.1 : 103640-35
- SunOS 5.5.1x86 : 103641-35
- SunOS 5.5 : 10261-08
- SunOS 5.5x86 : 103262-08

Ces correctifs sont disponibles à l'adresse :
http://sunsolve.sun.com/pub/securitypatches

6 Documentation

Bulletin de sécurité Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/210&type=0&nav=sec.sba

Gestion détaillée du document

29 octobre 2001 version initiale.