

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de vold 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-2002-AVI-150>

Gestion du document

Référence	CERTA-2002-AVI-150
Titre	Vulnérabilité de vold sous Solaris
Date de la première version	16 juillet 2002
Date de la dernière version	–
Source(s)	Avis de sécurité de Sun #45707
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

- Elévation de privilèges ;
- exécution de code arbitraire ;
- déni de service.

2 Systèmes affectés

Solaris 2.5.1, 2.6, 7 et 8 (architectures SPARC et Intel). La version 9 de Solaris n'est pas vulnérable.

3 Résumé

Un utilisateur mal intentionné peut provoquer un débordement de mémoire.

4 Description

vold (VOLume management Daemon) est un service permettant de monter automatiquement les médias amovibles tels que les lecteurs de disquettes ou les lecteurs de CD-ROMs.

Une vulnérabilité présente sur ce service permet à un utilisateur mal intentionné de provoquer un débordement de mémoire conduisant à une élévation de privilège ou à un déni de service.

Aucune trace dans les fichiers journaux ne permet de savoir si le système a subi ce type d'attaque, seul le service `vold` ne fonctionnera plus en cas d'échec.

5 Contournement provisoire

- Désactiver le montage automatique des médias amovibles en stoppant le service `vold` ;
- Renommer le script de démarrage du service `vold` de façon qu'il ne soit pas exécuté lors de la prochaine réinitialisation.

Les utilisateurs ne pourront plus 'monter' les médias amovibles, seul l'administrateur (`root`) en aura le pouvoir.

6 Solution

Appliquer le correctif correspondant à votre version de Solaris. Se référer au bulletin #45707 de sun (cf. section Documentation) pour connaître la version du correctif à appliquer.

7 Documentation

Bulletin de sécurité #45707 de Sun:

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F45707>

8 Gestion détaillée du document

16 juillet 2002 version initiale.