Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 octobre 2001
N° CERTA-2001-AVI-127

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Mac OS X

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-127

Gestion du document

Référence	CERTA-2001-AVI-127
Titre	Vulnérabilité sous Mac OS X
Date de la première version	24 octobre 2001
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

Elévation de privilèges.

2 Systèmes affectés

Mac OS X versions 10.01 à 10.04 et 10.1.

3 Résumé

Un utilisateur mal intentionné peut, à partir d'un accès à la console, obtenir les privilèges de l'administrateur *root*.

4 Description

Lors d'une session, un utilisateur mal intentionné peut, par une succession d'actions à la console (ouverture et fermeture de certaines applications), obtenir les privilèges de *root*. Cela est dû à une erreur dans la gestion des applications ayant le drapeau *setuid root* positionné.

Un scénario décrivant ces différentes étapes a été publié sur l'Internet.

5 Contournement provisoire

Une première solution consiste à terminer les sessions et à protéger l'accès physique à la machine. En effet, il est nécessaire d'avoir un accès à la console pour exploiter cette vulnérabilité.

Il est également possible de limiter l'exécution des programmes ayant le drapeau *setuid root* positionné. Pour identifier de telles applications, utiliser la commande suivante :

```
find / -perm -4000 -user root -print
```

Voici celles installées par défaut sur le système qui permettent d'exploiter cette vulnérabilité :

- /Applications/Utilities/Disk Utility.app/Contents/MacOS/Disk Utility
- /Applications/Utilities/NetInfo Manager.app/Contents/MacOS/Net Info Manager
- /Applications/Utilities/Print Center.app/Contents/MacOS/PrintingReset

Pour limiter à l'utilisateur *root* l'exécution de ces applications, il faut utiliser les commandes suivantes :

```
chmod go-x '/Applications/Utilities/Disk Utility.app/Contents/MacOS/Disk Utility'
chmod go-x '/Applications/Utilities/NetInfo Manager.app/Contents/MacOS/NetInfo Manager'
chmod go-x '/Applications/Utilities/Print Center.app/Contents/MacOS/PrintReset'
```

Pour limiter l'exécution de ces applications au groupe des administrateurs, il faut remplacer dans les lignes précédentes *chmod go-x* par *chmod o-x*.

6 Solution

Appliquer le correctif Apple par *Software Update* (menu *Pomme/Control Panels/Software Update*) ou le télécharger sur le site d'Apple :

http://docs.info.apple.com/article.html?artnum=120069

Gestion détaillée du document

24 octobre 2001 version initiale.