



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 août 2006
N° CERTA-2006-AVI-372

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dan Xsan Filesystem

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-2006-AVI-372>

Gestion du document

Référence	CERTA-2006-AVI-372
Titre	Vulnérabilité dan Xsan Filesystem
Date de la première version	25 août 2006
Date de la dernière version	-
Source(s)	Bulletin de sécurité Apple ID304188 du 14 août 2006
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

- Exécution de code arbitraire ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

Xsan Filesystem 1.x.

3 Résumé

Une vulnérabilité dans Xsan permet à un utilisateur local mal intentionné d'exécuter du code arbitraire avec le privilège du système.

4 Description

Une vulnérabilité de type débordement de mémoire est causée par une erreur dans le traitement des arborescences qui sont fournies au pilote de l'application Xsan Filesystem. Cette vulnérabilité peut être exploitée

par un utilisateur local ayant les droits en écriture à un volume `Xsan` afin de provoquer l'arrêt brutal du système ou d'exécuter du code arbitraire avec des privilèges élevés.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple du 14 août 2006 :
<http://docs.info.apple.com/article.html?artnum=304188>
- Mise à jour de sécurité Xsan Filesystem 1.4 pour Mac OS X 10.4 :
<http://www.apple.com/support/downloads/xsanfilesystem14formacosx104.html>
- Référence CVE CVE-2006-3506 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3506>

Gestion détaillée du document

25 août 2006 version initiale.