



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 avril 2005
N° CERTA-2005-AVI-150

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2005-AVI-150>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2005-AVI-150 |
| Titre | Multiples vulnérabilités dans Mac OS X |
| Date de la première version | 19 avril 2005 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Apple du 15 avril 2005 |
| Pièce(s) jointe(s) | |

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- élévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

- Mac OS X v10.3.8 ;
- Mac OS X Server v10.3.8.

3 Résumé

De nombreuses vulnérabilités permettent à un utilisateur local ou distant d'effectuer un déni de service, d'élèver ses privilèges ou d'exécuter du code arbitraire sur le système vulnérable.

4 Description

- CAN-2005-0969 : une vulnérabilité de type débordement de la mémoire permet à un utilisateur mal intentionné d'effectuer localement un déni de service ;
- CAN-2005-0970 : le système d'exploitation autorise par défaut la création et l'exécution de script SUID/SGID (hérité de FreeBSD), cette mise à jour de sécurité ne permet plus au système d'exploitation d'exécuter de tels scripts, pouvant être exploités par un individu mal intentionné afin d'élever ses privilèges ;
- CAN-2005-0971 : une vulnérabilité dans la fonction `semop()` de type débordement de mémoire permet à un utilisateur local mal intentionné d'élever ses privilèges ;
- CAN-2005-0972 : une vulnérabilité dans la fonction `searchfs()` de type débordement d'entier permet à un utilisateur local mal intentionné d'exécuter du code arbitraire sur le système avec des privilèges élevés ;
- CAN-2005-0973 : une vulnérabilité de la fonction `setsockopt()` permet à un individu local mal intentionné d'effectuer un déni de service en consommant toutes les ressources CPU du système ;
- CAN-2005-0974 : une vulnérabilité découverte dans la fonction `nfs_mount()` permet à un utilisateur local mal intentionné d'effectuer un déni de service ;
- CAN-2005-0975 : une vulnérabilité lors de l'analyse syntaxique de certains fichiers exécutables permet à un individu malveillant de figer temporairement le système vulnérable ;
- CAN-2005-0976 : une vulnérabilité présente dans l'application Safari permet à une personne mal intentionnée, au moyen d'un site web malicieusement construit d'exécuter du code JavaScript ou HTML dans le domaine local du système vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité d'Apple du 15 avril 2005 :
<http://docs.info.apple.com/article.html?artnum=301327>
- Mise à jour de sécurité Mac OS X Combined Update 10.3.9 :
<http://www.apple.com/support/downloads/macosxcombinedupdate1039.html>
- Mise à jour de sécurité Mac OS X Server Update 10.3.9 :
<http://www.apple.com/support/downloads/macosxserverupdate1039.html>
- Mise à jour de sécurité Mac OS X Server Update 10.3.9 Combo :
<http://www.apple.com/support/downloads/macosxserverupdate1039combo.html>
- Mise à jour de sécurité Mac OS X Update 10.3.9 :
<http://www.apple.com/support/downloads/macosxupdate1039.html>
- Référence CVE CAN-2005-0969 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0969>
- Référence CVE CAN-2005-0970 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0970>
- Référence CVE CAN-2005-0971 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0971>
- Référence CVE CAN-2005-0972 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0972>
- Référence CVE CAN-2005-0973 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0973>
- Référence CVE CAN-2005-0974 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0974>
- Référence CVE CAN-2005-0975 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0975>
- Référence CVE CAN-2005-0976 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0976>

Gestion détaillée du document

19 avril 2005 version initiale.