

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans certains clients FTP

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-2003-AVI-059>

Gestion du document

Référence	CERTA-2003-AVI-059
Titre	Vulnérabilité dans certains clients FTP
Date de la première version	25 mars 2003
Date de la dernière version	–
Source(s)	Vulnérabilité VU#258721 du CERT/CC
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 commandes arbitraires à distance.

2 Systèmes affectés

Certains clients FTP présents dans plusieurs systèmes :

- Mandrake ;
- RedHat ;
- SUN ;
- SCO ;
- IRIX.

3 Description

FTP (File Transfert Protocol) est un protocole client/serveur permettant l'échange de fichiers. Certains clients ont un problème dans la gestion des noms de fichiers débutant par un "pipe". Un individu mal intentionné possédant les droits d'administration sur le serveur peut créer un fichier avec un nom judicieusement choisi afin d'exécuter des commandes arbitraires lors de son téléchargement par un client FTP vulnérable.

4 Solution

Appliquer les correctifs fournis suivant la plate-forme et la version affectée (cf. Documentation).

5 Documentation

- Avis VU#258721 du CERT/CC :
<http://www.kb.cert.org/vuls/id/258721>
- Bulletin de sécurité Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKASA-2003:021>
- Bulletin de sécurité RedHat :
<http://rhn.redhat.com/errata/RHSA-2003-020.html>
- Bulletin de sécurité IRIX :
<ftp://patches.sgi.com/support/free/security/advisories/20030304-01-P>
- Bulletin de sécurité SCO :
<ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.3>
- Bulletin de sécurité SUN :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/50222>

Gestion détaillée du document

25 mars 2003 version initiale.