

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans file

---

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-2007-AVI-138>

---

### Gestion du document

Référence	CERTA-2007-AVI-138-004
Titre	Vulnérabilité dans file
Date de la première version	26 mars 2007
Date de la dernière version	01 août 2007
Source(s)	Mise à jour de file
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 à distance.

## 2 Systèmes affectés

file versions antérieures à 4.20.

## 3 Description

Une vulnérabilité de type débordement d'entier dans la fonction `file_printf` du programme `file` permet à une personne malintentionnée d'exécuter du code arbitraire à distance avec les droits de l'utilisateur.

## 4 Solution

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

## 5 Documentation

- Mise à jour de sécurité de file 4.20 du 02 mars 2007 :  
<http://mx.gw.com/pipermail/file/2007/000161.html>
- Bulletin de sécurité Gentoo GLSA-200703-26 du 30 mars 2007 :  
<http://www.gentoo.org/security/en/glsa/glsa-200703-26.xml>
- Bulletin de sécurité Gentoo GLSA-200705-25 du 31 mars 2007 :  
<http://www.gentoo.org/security/en/glsa/glsa-200705-25.xml>
- Bulletin de sécurité Ubuntu USN-439-1 du 21 mars 2007 :  
<http://www.ubuntu.com/usn/usn-439-1>
- Bulletin de sécurité SuSE SUSE-SR:2007:005 du 30 mars 2007 :  
[http://www.novell.com/linux/security/advisories/2007\\_5\\_sr.html](http://www.novell.com/linux/security/advisories/2007_5_sr.html)
- Bulletin de sécurité Redhat RHSA-2007-0124-2 du 23 mars 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-0124.html>
- Bulletin de sécurité Redhat RHSA-2007-0391-3 du 30 mai 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-0391.html>
- Bulletin de sécurité Mandriva MDKSA-2007:067 du 22 mars 2007 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:067>
- Bulletin de sécurité Debian DSA-1274-1 du 02 avril 2007 :  
<http://www.debian.org/security/2007/dsa-1274>
- Bulletin de sécurité Debian DSA-1343-1 du 31 juillet 2007 :  
<http://www.debian.org/security/2007/dsa-1343>
- Bulletin de sécurité Avaya ASA-2007-179 du 04 mai 2007 :  
<http://support.avaya.com/elmodocs2/security/ASA-2007-179.htm>
- Bulletin de sécurité FreeBSD-SA-07:04 du 23 mai 2007 :  
<http://security.freebsd.org/advisories/FreeBSD-SA-07:04.file.asc>
- Référence CVE CVE-2007-1536 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1536>
- Référence CVE CVE-2007-2799 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2799>

### Gestion détaillée du document

**26 mars 2007** version initiale.

**07 mai 2007** ajout des références Debian, Mandriva, SuSE, Gentoo, Avaya, Redhat, Ubuntu.

**29 mai 2007** ajout de la référence au bulletin de sécurité FreeBSD.

**01 juin 2007** ajout de la référence CVE et des références aux bulletins de sécurité Gentoo, RedHat.

**01 août 2007** ajout de la référence au bulletin de sécurité Debian.