

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans sendfile sous FreeBSD

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-2008-AVI-093>

Gestion du document

Référence	CERTA-2008-AVI-093
Titre	Vulnérabilité dans sendfile sous FreeBSD
Date de la première version	15 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD-SA-08:03.sendfile du 14 février 2008
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

FreeBSD 5.5 à 7.0.

3 Résumé

Une vulnérabilité dans *sendfile* sous FreeBSD permet à une personne malintentionnée de porter atteinte à la confidentialité des données.

4 Description

L'appel système *sendfile* sous FreeBSD permet à une application serveur de transmettre le contenu d'un fichier via une connexion réseau sans transiter par la mémoire de l'application.

Une vulnérabilité a été découverte : un processus peut ouvrir un fichier en écriture seule et utiliser *sendfile* pour envoyer son contenu via une connexion réseau. Une personne malintentionnée peut ainsi exploiter ceci pour accéder à des données qui sont confidentielles.

5 Solution

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

6 Documentation

- Bulletin de sécurité FreeBSD SA-08:03.sendfile du 14 février 2008 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-08:03.sendfile.asc>
- Référence CVE CVE-2008-0777 :
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-0777>

Gestion détaillée du document

15 février 2008 version initiale.