

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenBSD

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-113>

Gestion du document

Référence	CERTA-2007-AVI-113-001
Titre	Vulnérabilité dans OpenBSD
Date de la première version	09 mars 2007
Date de la dernière version	13 mars 2007
Source(s)	Bulletin de sécurité OpenBSD du 07 mars 2007
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

Déni de service à distance.

2 Systèmes affectés

OpenBSD versions 4.0 et antérieures.

3 Description

Une erreur dans la gestion de certains tampons dans le noyau du système d'exploitation OpenBSD permettrait à un utilisateur distant malintentionné de provoquer un dysfonctionnement du système. En particulier, le tampon impliqué dans la vulnérabilité (mbuf) est utilisé dans la mise en œuvre du protocole ICMPv6. Il serait donc possible de provoquer un déni de service par le biais d'un paquet ICMPv6 particulier.

4 Solution

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

5 Documentation

- Bulletin de sécurité de OpenBSD version 3.9 :
<http://www.openbsd.org/errata39.html>
- Bulletin de sécurité de OpenBSD version 4.0 :
<http://www.openbsd.org/errata40.html>

Gestion détaillée du document

09 mars 2007 version initiale ;

13 mars 2007 ajout du caractère distant de la vulnérabilité via un paquet ICMPv6.