Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 septembre 2004
N° CERTA-2004-AVI-298

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenBSD

Gestion du document

Référence	CERTA-2004-AVI-298
Titre	Vulnérabilité dans OpenBSD
Date de la première version	03 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité du 26 Août 2004 d'OpenBSD
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.

2 Systèmes affectés

OpenBSD versions 3.4 et 3.5.

3 Résumé

Une vulnérabilité a été découverte dans OpenBSD qui permet à un utilisateur mal intentionné d'effectuer un déni de service sur la machine vulnérable.

4 Description

Une vulnérabilité a été découverte dans la mise en œuvre du traitement des paquets ICMP par OpenBSD configuré en mode `bridge` et gérant le protocole IPsec. L'envoi d'un paquet ICMP malicieusement formé au travers du bridge permet à un utilisateur mal intentionné d'effectuer un déni de service sur la machine affectée.

5 Solution

Appliquer le correctif suivant la version d'OpenBSD :

- version 3.4 :
  ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/028_bridge.patch
- version 3.5 :
  ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/016_bridge.patch

6 Documentation

Bulletins de sécurité pour OpenBSD 3.4 et 3.5 du 26 Août 2004 :
http://www.openbsd.org/errata34.html#bridge
http://www.openbsd.org/errata.html#bridge

Gestion détaillée du document

03 septembre 2004 version initiale.