Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 avril 2004
N° CERTA-2004-AVI-140

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du noyau NetBSD

Gestion du document

Référence	CERTA-2004-AVI-140
Titre	Vulnérabilité du noyau NetBSD
Date de la première version	22 avril 2004
Date de la dernière version	–
Source(s)	Avis de sécurité NetBSD NetBSD-SA2004-006
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 ;
- injection de données dans un flux TCP.

2 Systèmes affectés

- NetBSD-current de sources antérieures au 22 avril 2004 ;
- NetBSD 1.5, 1.5.1, 1.5.2 et 1.5.3 ;
- NetBSD 1.6, 1.6.1 et 1.6.2 ;
- la branche NetBSD 2.0 est affectée mais la version finale NetBSD 2.0 incluera le correctif.

3 Résumé

Outre les faiblesses du protocole TCP (Transmission Control Protocol) connues depuis plusieurs années, une vulnérabilité dans la mise en oeuvre du protocole TCP par NetBSD permet à un utilisateur mal intentionné de créer un déni de service ou d'injecter des données dans un flux TCP.

4 Description

Le procole TCP, décrit dans la RFC 793, présente plusieurs faiblesses :

- Possibilité de fabriquer des paquets RST afin de terminer une connection TCP ;
- possibilité de fabriquer des paquets SYN afin de terminer une connection TCP ;
- possibilité d'injecter des paquets dans une session TCP.

En plus de ces faiblesses, la mise en oeuvre du protocole TCP dans le noyau 4.4BSD (dont NetBSD est dérivé) souffre d'un problème dans la validation des paquets TCP RST.

5 Solution

Appliquer le correctif fournit par NetBSD (cf. section Documentation).

6 Documentation

- Le protocole TCP (RFC 793) :
  http://www.ietf.org/rfc/rfc793.txt
- Considérations de sécurité sur le protocole TCP du 19 avril 2004 :
  http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-01.txt
- Avis de sécurité NetBSD NetBSD-SA2004-006 du 22 avril 2004 :
  ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc

Gestion détaillée du document

22 avril 2004 version initiale.