



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juillet 2005
N° CERTA-2005-AVI-241

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la pile TCP de 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-2005-AVI-241>

Gestion du document

Référence	CERTA-2005-AVI-241
Titre	Vulnérabilités dans la pile TCP de FreeBSD
Date de la première version	01 juillet 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'éditeur du
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

Toutes les versions de FreeBSD.

3 Description

Il a été découvert deux vulnérabilités dans la pile TCP de FreeBSD.

Lorsque la pile TCP reçoit un paquet contenant un marqueur de temps (timestamp), le contrôle du numéro de séquence n'est pas fait convenablement, ce qui permet à un attaquant d'augmenter de façon artificielle le marqueur horaire "recent" d'une connexion.

La seconde vulnérabilité permet à un attaquant de modifier certaines options TCP, via un paquet possédant le drapeau SYN positionné.

4 Solution

Appliquer les directives de l'éditeur (Cf. Documentation).

5 Documentation

- Bulletin de sécurité de FreeBSD du 29 juin 2005 :
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:15.tcp.asc>
- Références CVE CAN-2005-0356 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0356>
- Références CVE CAN-2005-2068 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2068>

Gestion détaillée du document

01 juillet 2005 version initiale.