Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juillet 2005
N° CERTA-2005-AVI-285

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité dans la mise en œuvre IPsec de FreeBSD



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-AVI-285 |
| Titre | Vulnérabilité dans la mise en œuvre IPsec de FreeBSD |
| Date de la première version | 28 juillet 2005 |
| Date de la dernière version | – |
| Source(s) | Avis de sécurité FreeBSD du 27 juillet 2005 |
| 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

FreeBSD 5.3 et FreeBSD 5.4.

## 3 Description

Une erreur dans la mise en œuvre d'IPsec dans FreeBSD, et plus particulièrement dans l'algorithme d'authentification AES-XCBXC-MAC, a pour conséquence qu'une même clé prédéfinie est toujours utilisée à un moment de l'algorithme, au lieu de la clé définie par l'administrateur. Cette erreur pourrait être utilisée par un individu distant malintentionné pour contourner la politique d'authentification.

## 4 Solution

Appliquer les directives de l'éditeur (cf. Section Documentation).

# 5 Documentation

- Bulletin de sécurité de FreeBSD du 27 juillet 2005 :
  ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:19.ipsec.asc
- Référence CVE CAN-2005-2359 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2359

# Gestion détaillée du document

**28 juillet 2005** version initiale.