

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans telnetd sur 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-2011-AVI-718>

---

### Gestion du document

Référence	CERTA-2011-AVI-718
Titre	Vulnérabilité dans telnetd sur FreeBSD
Date de la première version	26 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité de FreeBSD du 23 décembre 2011
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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Toutes les versions supportées de FreeBSD.

## 3 Résumé

Une vulnérabilité présente dans *telnetd* permet à une personne malintentionnée distante d'exécuter du code arbitraire avec les privilèges administrateur (*root*).

## 4 Description

Une vulnérabilité est présente dans *telnetd* sur FreeBSD. Elle permet à une personne malintentionnée distante d'exécuter du code arbitraire avec les privilèges administrateur (*root*).

La vulnérabilité est due à la clef de chiffrement fournie via le protocole *TELNET*, dont la longueur n'est pas validée avant qu'elle ne soit copiée dans un tampon de taille fixe.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité FreeBSD SA-11:08.telnetd du 23 décembre 2011 :  
<http://security.freebsd.org/advisories/FreeBSD-SA-11:08.telnetd.asc>
- Référence CVE CVE-2011-4862 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4862>

## **Gestion détaillée du document**

**26 décembre 2011** version initiale.