



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 19 juillet 2004  
N° CERTA-2004-AVI-234-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Faille dans le serveur SSLtelnet**

---

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-2004-AVI-234>

---

### Gestion du document

Référence	CERTA-2004-AVI-234-001
Titre	Faille dans le serveur SSLtelnet
Date de la première version	09 juillet 2004
Date de la dernière version	19 juillet 2004
Source(s)	Avis de sécurité iDefense
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 ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

Systèmes FreeBSD avec *SSLtelnet*, versions jusqu'à la version 0.13\_1.

## 3 Résumé

Une faille a été identifiée dans le code source du serveur *SSLtelnet*. Elle permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine hôte.

## 4 Description

*SSLtelnet* est un serveur *telnet* activant l'encapsulation de la communication dans un tunnel SSL/TLS. Il est lancé sur la machine hôte par l'intermédiaire du serveur *inetd*. Une faille liée à une mauvaise utilisation d'une chaîne de format peut être exploitée pour exécuter du code avec les privilèges du service - root dans la configuration installée -.

## 5 Contournement provisoire

- Arrêter le service en commentant la ou les ligne(s) concernée(s) dans le fichier de configuration du serveur *inetd* et en relançant ce dernier ;
- ou restreindre l'accès à ce service à des machines de confiance avec des règles de filtrage.

## 6 Solution

Ce serveur n'étant manifestement plus maintenu activement (disparition du site d'hébergement en 2000), il est fortement recommandé d'utiliser une autre solution.

## 7 Documentation

- Bulletin de sécurité iDefense :  
<http://www.iddefense.com/application/poi/display?id=114&type=vulnerabilities>
- Bulletin de sécurité Debian DSA-529 du 17 juillet 2004 :  
<http://www.debian.org/security/2004/dsa-529>
- Bulletin de sécurité FreeBSD pour SSLtelnet du 05 juillet 2004 :  
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-0640 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0640>

## Gestion détaillée du document

**09 juillet 2004** version initiale.

**19 juillet 2004** ajout des références aux bulletins de sécurité Debian et FreeBSD.