



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 juillet 2004  
N° CERTA-2004-AVI-245

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans FreeS/Wan, Openswan, StrongSwan et Super FreeS/Wan**

---

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-245>

---

### Gestion du document

Référence	CERTA-2004-AVI-245
Titre	Vulnérabilité dans FreeS/Wan, Openswan, StrongSwan et Super FreeS/Wan
Date de la première version	15 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Openswan
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Super FreeS/Wan 1.x, toutes les versions avec la mise à jour X.509 ;
- Openswan versions 1.x antérieures à la version 1.0.6 ;
- Openswan versions 2.x antérieures à la version 2.1.4 ;
- StrongSwan versions 2.x antérieures à la version 2.1.3 ;
- FreeS/Wan versions 1.x avec la mise à jour X.509 antérieures à la version 0.9.41 ;
- FreeS/Wan versions 2.x avec la mise à jour X.509 antérieures à la version 1.6.1 ;

## 3 Description

Une vulnérabilité présente dans une fonction de vérification des certificats X.509 (`verify_x509cert()`) permet à un utilisateur mal intentionné, via l'envoi d'un certificat malicieusement construit, de réaliser un déni de service ou de contourner la politique de sécurité.

## 4 Solution

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

## 5 Documentation

- Bulletin de sécurité Openswan du 28 juin 2004 :  
<http://www.openswan.org/support/vuln/can-2004-0590/>
- Bulletin de sécurité Gentoo du 25 juin 2004 :  
<http://security.gentoo.org/glsa/glsa-200406-20.xml>
- Bulletin de sécurité Mandrake du 14 juillet 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:070>
- Référence CVE CAN-2004-0590 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0590>

## Gestion détaillée du document

**15 juillet 2004** version initiale.