

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans SSH Tectia Server et Secure shell pour Windows

---

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-274>

---

### Gestion du document

Référence	CERTA-2005-AVI-274
Titre	Vulnérabilité dans SSH Tectia Server et Secure shell pour Windows
Date de la première version	20 juillet 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité SSH Communications Security RQ #11775
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Atteinte à la confidentialité des données.

## 2 Systèmes affectés

- SSH Tectia Server 4.x pour Microsoft Windows ;
- SSH Secure Shell pour Windows Servers 3.x.

Microsoft Windows permet à un utilisateur distant mal intentionné de porter atteinte à la confidentialité des données présentes sur le système.

## 3 Description

SSH est un protocole de communication permettant de chiffrer les informations émisent.

Une vulnérabilité découverte dans les applications SSH Tectia Server et SSH Secure Shell pour Microsoft Windows permet à un utilisateur local ou distant mal intentionné de porter atteinte à la confidentialité des données présentes sur le système.

Cette vulnérabilité est causée par une mauvaise gestion des droits appliqués sur le fichier contenant la clé d'identification du serveur.

## **4 Solution**

- Bulletin de sécurité SSH Communications Security RQ #11775 :  
<http://www.ssh.com/company/newsroom/article/653/>
- Référence CVE CAN-2005-2146 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2146>

## **5 Documentation**

### **Gestion détaillée du document**

**20 juillet 2005** version initiale.