

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans des mises à jour d'OpenSSH sous Red Hat

---

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-2008-AVI-428>

---

### Gestion du document

Référence	CERTA-2008-AVI-428-001
Titre	Vulnérabilités dans des mises à jour d'OpenSSH sous Red Hat
Date de la première version	22 août 2008
Date de la dernière version	29 août 2008
Source(s)	Annonce de sécurité Red Hat RHSA-2008:0855-6 du 22 août 2008
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

Certains paquets de mises à jour OpenSSH distribués pour Red Hat Desktop et Red Hat Enterprise.

## 3 Description

Certains serveurs concernant la distribution de paquets pour Red Hat auraient été compromis. Il est possible que certaines mises à jour, en particulier concernant OpenSSH, ne soient pas correctes. Aucune information sur la date de compromission n'est à ce jour connue.

Red Hat publie avec une nouvelle signature les paquets OpenSSH qui corrigent la vulnérabilité CVE-2007-4752 décrite dans l'avis CERTA-2007-AVI-497.

Un script est également fourni afin de tester sur les systèmes les versions installées. Il indique, en s'appuyant sur une liste noire de signatures pas nécessairement exhaustive, si des versions frauduleuses sont présentes.

## 4 Solution

Se référer au bulletin de sécurité RHSA-2008-0855 de Red Hat pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Bulletin de sécurité RedHat RHSA-2008:0855 du 22 août 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0855.html>
- Référence CVE CVE-2007-4752 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4752>
- Référence CVE CVE-2008-3844 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3844>
- Script de test fourni par Red Hat :  
<http://www.redhat.com/security/data/openssh-blacklist.html>
- Avis de sécurité CERTA-2007-AVI-497 du 14 novembre 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-497/>

## Gestion détaillée du document

**22 août 2008** version initiale.

**29 août 2008** ajout du CVE spécifique pour l'incident.