

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Apache Subversion

---

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-327>

---

### Gestion du document

Référence	CERTA-2011-AVI-327
Titre	Multiples vulnérabilités dans Apache Subversion
Date de la première version	03 juin 2011
Date de la dernière version	–
Source(s)	Notes de sécurité Apache Subversion n° CVE-2011-1752, CVE-2011-1783 et CVE-2011-1921
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 à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

Module `mod_dav_svn` pour Apache HTTPD versions 1.5.0 à 1.6.16.

## 3 Résumé

Trois vulnérabilités ont été corrigées dans le module Subversion du serveur Apache. L'une d'entre-elles permet à un attaquant de réaliser un déni de service à distance.

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans la version 1.6.17 du module Subversion `mod_dav_svn` pour le serveur Apache:

- un déréférencement de pointeur NULL permet à une personne malveillante d'arrêter le serveur de manière inopinée (CVE-2011-1752) ;

- dans certaines configurations du serveur, un attaquant peut réaliser un déni de service en utilisant des requêtes spécialement conçues qui font entrer le programme dans une boucle infinie (CVE-2011-1783) ;
- dans certaines configurations du serveur, un utilisateur peut accéder au contenu des fichiers de manière illégitime (CVE-2011-1921).

## 5 Solution

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

## 6 Documentation

- Note de sécurité Apache Subversion n° CVE-2011-1752 :  
<http://subversion.apache.org/security/CVE-2011-1752-advisory.txt>
- Note de sécurité Apache Subversion n° CVE-2011-1783 :  
<http://subversion.apache.org/security/CVE-2011-1783-advisory.txt>
- Note de sécurité Apache Subversion n° CVE-2011-1921 :  
<http://subversion.apache.org/security/CVE-2011-1921-advisory.txt>
- Référence CVE CVE-2011-1752 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1752>
- Référence CVE CVE-2011-1783 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1783>
- Référence CVE CVE-2011-1921 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1921>

## Gestion détaillée du document

**03 juin 2011** version initiale.