



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2004
N° CERTA-2004-AVI-329-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2004-AVI-329>

Gestion du document

Référence	CERTA-2004-AVI-329-001
Titre	Vulnérabilité dans Subversion
Date de la première version	30 septembre 2004
Date de la dernière version	08 octobre 2004
Source(s)	Bulletin de sécurité Subversion
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

- Toutes les versions de Subversion antérieures à 1.0.7 incluse ;
- les versions candidates 1.1-rc1, rc2 et rc3.

3 Résumé

Une vulnérabilité du module Apache mod_authz_svn de Subversion permet à un utilisateur mal intentionné de contourner la politique de sécurité mise en place par l'administrateur.

4 Description

Subversion est un système de contrôle des versions de fichier, ajoutant des fonctionnalités à CVS (Concurrent Versions System) telle la possibilité de copier, déplacer ou effacer des fichiers ou répertoires. Un serveur Subversion peut être mis en place à partir d'un module Apache, d'un service autonome (svnserver) ou à la

demande encapsulé dans le protocole SSH. Le module Apache `mod_authz_svn` limite les accès aux répertoires gérés par `Subversion`. Une vulnérabilité présente dans le module Apache `mod_authz_svn` permet à un utilisateur mal intentionné d'accéder à des répertoires dont les droits restreignent l'accès.

5 Solution

Mettre à jour `Subversion` avec la version 1.0.8 ou 1.1.0-rc4 :
http://subversion.tigris.org/project_packages.html

6 Documentation

- Bulletin de sécurité `Subversion` :
<http://subversion.tigris.org/security/CAN-2004-0749-advisory.txt>
- Bulletin de sécurité Gentoo GLSA 200409-35 du 29 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-35.xml>
- Référence CVE CAN-2004-0749 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0749>

Gestion détaillée du document

30 septembre 2004 version initiale.

08 octobre 2004 ajout référence au bulletin de sécurité de Gentoo.