Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juillet 2004
N° CERTA-2004-AVI-256

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de subversion

Gestion du document

Référence	CERTA-2004-AVI-256
Titre	Vulnérabilité de subversion
Date de la première version	28 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA 200407-20
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

`subversion` versions 1.0.5 et versions antérieures.

3 Résumé

Une vulnérabilité du module Apache `mod_authz_svn` inclus dans `subversion` permet à un utilisateur mal intentionné de contourner la politique de sécurité.

4 Description

`subversion` est un système de contrôle des versions de fichiers, 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` fonctionne avec `subversion` afin de limiter les accès aux répertoires gérés par `subversion` en fonction d'une politique de sécurité définie par l'administrateur.
Une vulnérabilité du module Apache `mod_authz_svn` permet à un utilisateur d'écrire dans des répertoires non autorisés.

5 Contournement provisoire

- Désactiver le module Apache `mod_authz_svn` (utiliser le serveur `svnserve` à la place) ;
- garder les données sensibles dans des emplacements séparés des répertoires gérés par `subversion`.

6 Solution

- A partir des sources, mettre à jour `subversion` en version 1.0.6 ;
  http://subversion.tigris.org/tarballs/subversion-1.0.6.tar.bz2
- se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site Internet de subversion :
  http://subversion.tigris.org
- Bulletin de sécurité subversion :
  http://subversion.tigris.org/security/mod_authz_svn-copy-advisory.txt
- Liste des changements dans subversion :
  http://svn.collab.net/repos/svn/tags/1.0.6/CHANGES
- Bulletin de sécurité Gentoo GLSA 200407-20 du 26 juillet 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200407-20.xml
- Mise à jour de sécurité du paquetage NetBSD ap2-subversion :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/ap2-subversion/README.html

Gestion détaillée du document

28 juillet 2004 version initiale.