Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2007
N° CERTA-2007-AVI-383

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Subversion (svn)

Gestion du document

Référence	CERTA-2007-AVI-383
Titre	Vulnérabilité dans Subversion (svn)
Date de la première version	30 août 2007
Date de la dernière version	–
Source(s)	Annonce de la version 1.4.5 de Subversion le 27 août 2007
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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Subversion, pour les versions antérieures à 1.4.5.

3 Résumé

Une vulnérabilité a été identifiée dans l'application de gestion de versions Subversion (aussi écrit en abrégé `svn`). Elle permettrait à une personne malveillante, sous certaines conditions, d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans l'application de gestion de versions Subversion (aussi écrit en abrégé `svn`). Le concept, similaire à `CVS`, repose sur un dépôt centralisé. Il offre aux clients un ensemble de commandes, incluant `checkout` (`co`) et `update` (`up`).

Cependant, des bibliothèques installées chez le client permettrait de créer des fichiers sur le poste, pendant l'une de ces opérations, même si le fichier ne se trouve pas dans le contexte de la copie de travail `svn`.

Une personne malveillante distante pourrait ainsi profiter de cette vulnérabilité pour écraser des fichiers existants, et exécuter des commandes arbitraires sur le système du client vulnérable.

5 Solution

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

6 Documentation

- Annonce de la vulnérabilité par le laboratoire CRISP :
  http://crisp.cs.du.edu/q=node/36
- Annonce du changement de version Subversion le 27 août 2007 :
  http://subversion.tigris.org/servlets/NewsItemView?newsItemID=1941
- Détails du changement de version Subversion publiés le 28 août 2007 :
  http:///subversion.tigris.org/servlets/ReadMsg?list=users&msgNo=69413
- Référence CVE CVE-2007-3846 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3846

Gestion détaillée du document

30 août 2007 version initiale.