

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-197>

Gestion du document

Référence	CERTA-2004-AVI-197-001
Titre	Vulnérabilité de subversion
Date de la première version	14 juin 2004
Date de la dernière version	17 juin 2004
Source(s)	Avis de sécurité Gentoo GLSA-200406-07
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de `subversion` antérieures à la version 1.0.5.

3 Résumé

Une vulnérabilité dans `subversion` permet à un utilisateur mal intentionné de créer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

`subversion` est un système client/serveur utilisé pour la gestion des versions de fichiers essentiellement textuels.

Le service `svnserve` permet un accès aux fichiers gérés par `subversion` en utilisant une URI (Uniform Resource Identifier) du type `svn://`, `svn+ssh://` ou `svn+*://` (tunnels).

Une mauvaise gestion de la longueur de l'URI envoyée par le client permet à un utilisateur mal intentionné de créer un déni de service ou d'exécuter du code arbitraire à distance avec les privilèges du service `svnserve`.

5 Solution

Se référer à la section Documentation pour l'obtention des correctifs.

La version 1.0.5 de `subversion` corrige cette vulnérabilité.

La dernière version de `subversion` est téléchargeable à l'adresse :

http://subversion.tigris.org/project_packages.html

6 Documentation

- Site Internet de `subversion` :
<http://subversion.tigris.org>
- Avis de sécurité `subversion` :
<http://subversion.tigris.org/security/CAN-2004-0413-advisory.txt>
- Avis de sécurité Gentoo GLSA-200406-07 du 10 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-07.xml>
- Avis de sécurité Suse SUSE-SA:2004:018 du 17 juin 2004 :
http://www.suse.com/de/security/2004_18_subversion.html
- Mise à jour du paquetage NetBSD `subversion` :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/devel/subversion/README.html>
- Référence CVE CAN-2004-0413 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0413>

Gestion détaillée du document

14 juin 2004 version initiale.

17 juin 2004 ajout référence à l'avis de sécurité de Suse.