Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 janvier 2004
N° CERTA-2003-AVI-216-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faille dans le serveur CVS

Gestion du document

Référence	CERTA-2003-AVI-216-002
Titre	Faille dans le serveur CVS
Date de la première version	22 décembre 2003
Date de la dernière version	14 janvier 2004
Source(s)	–
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

Créations de répertoires et fichiers arbitraires.

2 Systèmes affectés

Tout système hébergeant un serveur CVS en version 1.11.9 et antérieures.

3 Résumé

Il est possible de demander au serveur CVS de tenter de créer des répertoires et éventuellement des fichiers dans la racine du système hôte.

4 Description

CVS est un système client/serveur de contrôle de versions. Il est en particulier utilisé pour gérer les sources des logiciels en développement. Un utilisateur mal intentionné peut envoyer des requêtes malicieuses qui seront mal interprétées par le serveur qui tentera alors de créer des fichiers en dehors de son arborescence.

5 Contournement provisoire

Les droits de la racine ne permettent usuellement pas au compte utilisateur du serveur CVS de créer des fichiers. Vérifier que c'est le cas et éventuellement modifier les droits.

6 Solution

Mettre à jour.

- Sources en version 1.11.10 au moins :
  http://ccvs.cvshome.org/servlets/ProjectDownloadList
- Mandrake Linux :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:112
- Slackware Linux :
  http://www.slackware.com/lists/archive/viewer.php?l=slackware-security&y=2003&m=slackware-security.402538
- Gentoo :
  http://www.securityfocus.com/advisories/6161
- Red Hat :
  http://rhn.redhat.com/errata/RHSA-2004-003.html
- Debian :
  http://www.debian.org/security/2004/dsa-422

7 Documentation

Référence CVE CAN-2003-0977 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0977

Gestion détaillée du document

22 décembre 2003 version initiale.
13 janvier 2004 Ajout référence aux bulletins de sécurité de Gentoo et Red Hat.
14 janvier 2004 Ajout référence au bulletin de sécurité de Debian.