Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2005
N° CERTA-2005-AVI-341

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'outil de développement CVS

Gestion du document

Référence	CERTA-2005-AVI-341
Titre	Vulnérabilité de l'outil de développement CVS
Date de la première version	09 septembre 2005
Date de la dernière version	–
Source(s)	Avis de sécurité Linux Red Hat
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

Usurpation locale de privilèges.

2 Systèmes affectés

Tout système Unix avec un serveur CVS.

3 Résumé

Un utilisateur local mal intentionné peut faire exécuter des commandes arbitraires avec les privilèges d'une victime lançant la commande `cvsbug`.

4 Description

CVS (« Concurrent Versions System ») est un système client/serveur pour la gestion des versions de fichiers.

`cvsbug` est un script écrit en shell Unix permettant à un utilisateur quelconque de remonter aux développeurs de CVS un bogue quelconque.

Une mauvaise gestion des fichiers temporaires peut être détournée pour écraser des fichiers accessibles en écriture à l'utilisateur exécutant `cvsbug`.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site internet de CVS :
  http://www.nongnu.org/cvs/
- Bulletin de sécurité RedHat RHSA-2005:756 du 06 septembre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-756.html
- Linux Fedora :
  - Mise à jour de sécurité pour Fedora Core 3 du 23 août 2005 :
    http://www.securityfocus.com/advisories/9114
  - Mise à jour de sécurité pour Fedora Core 4 du 23 août 2005 :
    http://www.securityfocus.com/advisories/9113
- Debian Linux :
  - Bulletin de sécurité Debian DSA-802 du 07 septembre 2005 (cvs) :
    http://www.debian.org/security/2005/dsa-802
  - Bulletin de sécurité Debian DSA-806 du 09 septembre 2005 (gcvs) :
    http://www.debian.org/security/2005/dsa-806
- Bulletin de sécurité FreeBSD SA-05-20 pour CVS du 07 septembre 2005 :
  ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:20.cvsbug.asc

Gestion détaillée du document

09 septembre 2005 version initiale.