

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans CVS

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-2005-AVI-167>

Gestion du document

Référence	CERTA-2005-AVI-167-001
Titre	Multiples vulnérabilités dans CVS
Date de la première version	17 mai 2005
Date de la dernière version	11 juillet 2005
Source(s)	Bulletin de sécurité RedHat RHSA-2005-387
Pièce(s) jointe(s)	

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.

2 Systèmes affectés

Concurrent Versions System (CVS) 1.x.

3 Description

CVS (“Concurrent Versions System”) est un système client/serveur utilisé pour la gestion des versions de fichiers essentiellement textuels.

Quatre vulnérabilités découvertes dans l'application CVS permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou d'effectuer un déni de service.

4 Solution

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

La mise à jour CVS 1.11.20 est disponible à l'adresse suivante :
<http://ccvs.home.org/servlets/ProjectsDocumentList>

5 Documentation

- Site Internet de l'éditeur :
<http://www.cvshome.org>
- Bulletin de sécurité Gentoo GLSA 200504-16/CVS du 22 avril 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200504-16.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:073 du 20 avril 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA2005:073>
- Bulletin de sécurité RedHat RHSA-2005:387 du 25 avril 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-387.html>
- Mise à jour de sécurité pour Fedora Core 2 pour CVS :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité pour Fedora Core 3 pour CVS :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité FreeBSD FreeBSD-SA-05:05.cvs du 22 avril 2005 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:05.cvs.asc>
- Bulletin de sécurité OpenBSD #016 du 28 avril 2005 :
<http://www.openbsd.org/errata.html#cvms>
- Bulletin de sécurité SUSE SUSE-SA:2005:024 du 18 avril 2005 :
http://www.novell.com/linux/security/advisories/2005_24_cvs.html
- Bulletin de sécurité Debian DSA-742 du 07 juillet 2005 :
<http://www.debian.org/security/2005/dsa-742>
- Référence CVE CAN-2005-0753 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0753>

Gestion détaillée du document

17 mai 2005 version initiale.

11 juillet 2005 ajout des références aux bulletins de sécurité SUSE et Debian.