

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2004-AVI-130>

Gestion du document

Référence	CERTA-2004-AVI-130-004
Titre	Vulnérabilité du client CVS
Date de la première version	15 avril 2004
Date de la dernière version	10 mai 2004
Source(s)	Bulletin de sécurité SuSE-SA:2004:008 de SuSE Bulletin de sécurité RHSA-2004:154 de Red Hat Bulletin de sécurité MDKSA-2004:028 de Mandrake Bulletin de sécurité GLSA 200404-13 de Gentoo
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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Version de CVS 1.11.14 et antérieures.

3 Résumé

Une vulnérabilité présente dans le client CVS peut permettre, sous certaines conditions, de réaliser la prise de contrôle à distance d'un système vulnérable. Une vulnérabilité est également présente dans le serveur CVS. L'exploitation de cette vulnérabilité permet de récupérer des fichiers hors de l'arborescence du serveur CVS.

4 Description

CVS (Concurrent Versions System) est un système client/serveur pour la gestion des versions de fichiers. Un individu mal intentionné peut maintenir un serveur CVS malicieux renvoyant des noms de fichiers avec un chemin d'accès absolu et non relatif. Un utilisateur réalisant une opération de chargement d'un fichier depuis ce serveur au moyen d'un client CVS vulnérable pourra alors, à son insu, écraser ou installer un fichier arbitraire sur sa machine.

Une vulnérabilité est également présente dans le serveur CVS. Un client peut, en spécifiant des chemins d'accès relatifs contenant la chaîne de caractères ". . /", accéder à des fichiers RCS situés en dehors de l'arborescence du serveur CVS (\$CVSROOT).

5 Solution

Installer la version 1.11.15 de CVS ou appliquer les correctifs des éditeurs :

- Bulletin de sécurité SuSE-SA:2004:008 de SuSE :
http://www.suse.com/de/security/2004_08_cvs.html
- Bulletin de sécurité RHSA-2004:153 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-153.html>
- Bulletin de sécurité RHSA-2004:154 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-154.html>
- Bulletin de sécurité MDKSA-2004:028 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:028>
- Bulletin de sécurité GLSA 200404-13 de Gentoo :
<http://www.gentoo.org/security/en/glsa/glsa-200404-13.xml>
- Bulletin de sécurité FreeBSD-SA-04:07.cvs de FreeBSD :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:07.cvs.asc>
- Bulletin de sécurité DSA-486 de Debian :
<http://www.debian.org/security/2004/dsa-486>
- Correctifs de sécurité pour OpenBSD 3.3, OpenBSD 3.4 et OpenBSD 3.5 :
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/002_cvs.patch
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/017_cvs.patch
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.3/common/022_cvs.patch
- Bulletin de sécurité SGI 20040404-01-U du 21 avril 2004 :
<ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc>

6 Documentation

- Annonce de la sortie de la version 1.11.15 de CVS :
<http://www.cvshome.org>
- Référence CVE CAN-2004-0180 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0180>
- Référence CVE CAN-2004-0405 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0405>

7 Documentation

Gestion détaillée du document

15 avril 2004 version initiale.

16 avril 2004 mention de la vulnérabilité de type "directory traversal" sur le serveur CVS ; ajout du bulletin de sécurité de FreeBSD.

19 avril 2004 ajout de la référence CVE CAN-2004-0405 et du bulletin de sécurité de Debian.

05 mai 2004 ajout des références aux correctifs de sécurité pour OpenBSD.

10 mai 2004 ajout des références aux bulletins de sécurité RedHat et SGI.