

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur 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-170>

Gestion du document

Référence	CERTA-2004-AVI-170-002
Titre	Vulnérabilité du serveur CVS
Date de la première version	21 mai 2004
Date de la dernière version	15 juin 2004
Source(s)	Avis de sécurité eMatters
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

- Elévation de privilèges ;
- exécution de code arbitraire à distance.

2 Systèmes

Les versions de CVS égales ou antérieures à la version 1.11.15 (branche stable) sont affectées.

3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans la partie serveur de CVS (“Concurrent Versions System”) peut être exploitée par un utilisateur mal intentionné afin d’exécuter du code arbitraire à distance sur une machine hébergeant un serveur CVS vulnérable.

4 Description

CVS (“Concurrent Versions System”) est un système client/serveur utilisé pour la gestion des versions de fichiers essentiellement textuels. A cause d’une erreur de programmation dans l’analyse des données reçues, il est

possible, à l'aide d'une ligne "Entry" habilement construite, d'écrire au-delà de la mémoire allouée. Cela peut être exploité pour exécuter du code avec les privilèges du serveur.

5 Solution

Mettre à jour le serveur (version source 1.11.16) en suivant les recommandations de l'éditeur.

- Avis de sécurité Debian GNU/Linux DSA-505 du 19 mai 2004 :
<http://www.debian.org/security/2004/dsa-505>
- Avis de sécurité Mandrake Linux MDKSA-2004:048 du 19 mai 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:048>
- Avis de sécurité Red Hat Linux RHSA-2004:190 du 19 mai 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-190.html>
- Avis de sécurité SUSE Linux SuSE-SA:2004:013 du 19 mai 2004 :
http://www.suse.com/de/security/2004_13_cvs.html
- Avis de sécurité Gentoo Linux GLSA-200405-12 du 20 mai 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200405-12.xml>
- Avis de sécurité FreeBSD FreeBSD-SA-04:10.cvs du 19 mai 2004 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:10.cvs.asc>
- Avis de sécurité OpenBSD du 20 mai 2004 :
<http://www.openbsd.org/errata.html>
- Avis de sécurité NetBSD du 21 mai 2004 :
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-008.txt.asc>

6 Documentation

- Site Internet de CVS :
<http://www.cvshome.org>
- Avis de sécurité d'eMatters :
<http://security.e-matters.de/advisories/072004.html>
- Note de vulnérabilité de l'US CERT :
<http://www.kb.cert.org/vuls/id/192038>
- Référence CVE CAN-2004-0396 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0396>

Gestion détaillée du document

21 mai 2004 version initiale.

24 mai 2004 corrections de liens et ajout de la référence NetBSD.

15 juin 2004 modification de la référence NetBSD.