



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juin 2004
N° CERTA-2004-AVI-190-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-190>

Gestion du document

Référence	CERTA-2004-AVI-190-003
Titre	Vulnérabilités de CVS
Date de la première version	10 juin 2004
Date de la dernière version	15 juin 2004
Source(s)	Bulletin de sécurité "More CVS remote vulnerabilities" d'e-matters
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

- Exécution de code arbitraire à distance ;
- déni de service.

2 Systèmes affectés

- Les versions de CVS égales ou antérieures à la version 1.11.16 (branche stable) sont affectées ;
- les versions de CVS égales ou antérieures à la version 1.12.8 (branche de développement) sont affectées.

3 Description

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

Un audit de code a révélé que de nombreuses vulnérabilités de type débordement de mémoire sont présentes dans le code du serveur CVS.

Un utilisateur mal intentionné peut utiliser ces vulnérabilités afin de réaliser un déni de service ou l'exécution de code arbitraire, à distance, sur une plate-forme vulnérable.

4 Solution

Les versions 1.11.17 ou 1.12.9 disponibles sur le site CVS (cf. section Documentation) corrigent ces vulnérabilités.

5 Documentation

- site Internet de CVS :
<http://www.cvshome.org>
- Avis de sécurité d’eMatters :
<http://security.e-matters.de/advisories/092004.html>
- Bulletin de sécurité MDKSA-2004:058 de Mandrake du 09 juin 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:058>
- Bulletin de sécurité SuSE-SA:2004:015 de SuSE du 09 juin 2004 :
http://www.suse.com/de/security/2004_15_cvs.html
- Bulletin de sécurité RHSA-2004:233 de Red Hat du 09 juin 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-233.html>
- Avis de sécurité DSA-517 de Debian du 10 juin 2004 :
<http://www.debian.org/security/2004/dsa-517>
- Avis de sécurité DSA-519 de Debian du 15 juin 2004 :
<http://www.debian.org/security/2004/dsa-519>
- Avis de sécurité GLSA-200406-06 de Gentoo du 10 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-06.xml>
- Avis de sécurité OpenBSD pour CVS du 09 juin 2004 :
<http://www.openbsd.org/errata.html>
- Mise à jour de sécurité du paquetage NetBSD cvs :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/devel/cvs/README.html>
- Référence CVE CAN-2004-0414 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0414>
- Référence CVE CAN-2004-0416 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0416>
- Référence CVE CAN-2004-0417 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0417>
- Référence CVE CAN-2004-0418 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0418>

10 juin 2004 version initiale.

11 juin 2004 ajout des références aux bulletins de Debian et Gentoo.

14 juin 2004 ajout de la référence à la mise à jour de NetBSD.

15 juin 2004 ajout de la référence au bulletin de sécurité Debian.