Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 7 février 2003
N° CERTA-2003-AVI-008-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de CVS

Gestion du document

Référence	CERTA-2003-AVI-008-002
Titre	Vulnérabilité de CVS
Date de la première version	21 janvier 2003
Date de la dernière version	7 février 2003
Source(s)	Bulletin de sécurité "CVS remote vulnerability" 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

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

2 Systèmes affectés

Les versions de CVS égales ou antérieures à la version 1.11.4 sont affectées.

3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans 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 est un outil dédié à la gestion des codes sources.

Par le biais d'un nom de répertoire habilement constitué, un utilisateur mal intentionné peut exploiter une vulnérabilité présente dans le serveur CVS afin de réaliser une élévation de privilèges.

Via les commandes `Update-prog` et `Checkin-prog` du serveur CVS, il est alors possible d'exécuter des commandes avec les privilèges du serveur CVS.

Cette vulnérabilité est exploitable sans authentification préalable sur des serveurs CVS offrant des connexions anonymes, même si l'accès n'est autorisé qu'en lecture seule.

5 Solution

La version 1.11.5 de CVS corrige cette vulnérabilité.

6 Documentation

- Site de CVS :
  http://ccvs.cvshome.org/servlets/NewsItemView?newsID=51
- Bulletin de sécurité "CVS remote vulnerability" d'e-matters :
  http://security.e-matters.de/advisories/012003.html
- Bulletin de sécurité RHSA-2003:012 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-012.html
- Bulletin de sécurité MDKSA-2003:009 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:009
- Bulletin de sécurité DSA-233 de Debian :
  http://www.debian.org/security/2003/dsa-233
- Bulletin de sécurité d'OpenBSD du 20 janvier 2003 :
  http://www.openbsd.org/security.html
- Bulletin de sécurité SuSE-SA:2003:0007 de SuSE :
  http://www.suse.com/de/security/2003_007_cvs.html
- Avis de sécurité CA-2003-02 du CERT/CC :
  http://www.cert.org/advisories/CA-2003-02.html
- Avis de sécurité FreeBSD-SA-03:01.cvs de FreeBSD :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:01.cvs.asc
- Avis de sécurité #50439 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50439

Gestion détaillée du document

21 janvier 2003 version initiale.
23 janvier 2003 ajout références aux avis de SuSE et du CERT/CC.
07 février 2003 ajout références aux avis de FreeBSD et de SUN.