

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2005-AVI-374>

Gestion du document

Référence	CERTA-2005-AVI-374
Titre	Vulnérabilité de CVS
Date de la première version	04 octobre 2005
Date de la dernière version	–
Source(s)	Mise à jour de sécurité de CVS
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

Concurrent Versions System (CVS) version 1.12.12 et versions antérieures.

3 Description

Deux vulnérabilités ont été identifiées dans CVS. Ces vulnérabilités sont dues à des erreurs au niveau de la bibliothèque `zlib` (cf. avis du CERTA : CERTA-2005-AVI-276).

L'exploitation de ces deux vulnérabilités permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.

4 Solution

La version 1.12.13 de CVS corrige ces vulnérabilités.

5 Documentation

- Site de l'éditeur :
<http://www.nongnu.org/cvs/>
- Mise à jour de sécurité :
<http://www.nongnu.org/cvs/#TOCdownloading>
- Références CVE : CAN-2005-2096
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2096>

Gestion détaillée du document

04 octobre 2005 version initiale.