



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 décembre 2004
N° CERTA-2004-AVI-416

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Xine

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-416>

Gestion du document

Référence	CERTA-2004-AVI-416
Titre	Vulnérabilités dans Xine
Date de la première version	22 décembre 2004
Date de la dernière version	–
Source(s)	Avis de sécurité sur le site de Xine
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.

2 Systèmes affectés

Xine versions 0.99.2 et antérieures.

3 Résumé

Deux vulnérabilités affectant Xine permettent l'exécution de code arbitraire à distance.

4 Description

Xine est un lecteur multimedia pour les plates-formes Unix.

Deux vulnérabilités de type débordement de tampon ont été découvertes dans la gestion des entrées de type `pnm://`. Un utilisateur mal intentionné peut, par le biais d'un serveur malicieux, exécuter du code arbitraire à distance.

5 Solution

Se référer au site de Xine pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de Xine :
<http://xinehq.de>
- Bulletin de sécurité 176 d'iDefense du 21 décembre 2004 :
<http://www.idefense.com/application/poi/display?id=176&type=vulnerabilities>
- Bulletin de sécurité 177 d'iDefense du 21 décembre 2004 :
<http://www.idefense.com/application/poi/display?id=177&type=vulnerabilities>
- Référence CVE CAN-2004-1187 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1187>
- Référence CVE CAN-2004-1188 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1188>

Gestion détaillée du document

22 décembre 2004 version initiale.