



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2005
N° CERTA-2005-AVI-004-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2005-AVI-004>

Gestion du document

Référence	CERTA-2005-AVI-004-002
Titre	Vulnérabilité dans Xine
Date de la première version	04 janvier 2005
Date de la dernière version	25 janvier 2005
Source(s)	Bulletin de sécurité XSA-2004-7 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

- Toutes les versions 1-alpha ;
- toutes les versions 1-beta ;
- toutes les versions 1-rc.

Les versions antérieures à la versions 1-alpha0 ainsi que les version 1.0 et ultérieures sont non affectées.

3 Résumé

Une vulnérabilité dans le démultiplexeur AIFF de Xine permet l'exécution de code arbitraire à distance.

4 Description

AIFF (Audio Interchange File Format) est un format de fichier reconnu par la bibliothèque `xine-lib`.

Une vulnérabilité est présente dans la routine de traitement des en-têtes de fichiers au format AIFF dans `xine`. Un utilisateur mal intentionné peut provoquer l'exécution de code arbitraire à distance, par le biais d'un fichier ou d'un site web habilement constitués.

L'exploitation de cette vulnérabilité ne se limite pas aux fichiers AIFF, car le démultiplexeur AIFF peut être utilisé pour traiter des fichiers qui ne sont pas au format AIFF.

5 Solution

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

6 Documentation

- Site de Xine :
<http://xinehq.de>
- Référence CVE CAN-2004-1300 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1300>
- Bulletin de sécurité FreeBSD « libxine – buffer-overflow vulnerability in aiff support » du 29 décembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité Gentoo GLSA-200501-07 du 06 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-07.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:011 du 19 janvier 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:011>

Gestion détaillée du document

04 janvier 2005 version initiale.

07 janvier 2005 ajout référence au bulletin de sécurité Gentoo GLSA-200501-07.

25 janvier 2005 ajout référence au bulletin de sécurité Mandrake MDKSA-2005:011.