Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2005
N° CERTA-2005-AVI-388-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque multimedia xine-lib

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-388

Gestion du document

Référence	CERTA-2005-AVI-388-001
Titre	Vulnérabilité de la bibliothèque multimedia xine-lib
Date de la première version	10 octobre 2005
Date de la dernière version	12 octobre 2005
Source(s)	
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

Tout système avec un lecteur multimedia utilisant la bibliothèque *xine-lib* avec des sources non corrigées en versions :

- supérieures ou égales à 1-beta3 pour les 1-beta,
- toutes les versions 1-rc,
- 1.0 à 1.0.2,
- 1.1.0.

3 Résumé

Une vulnérabilité dans l'interprétation des réponses CDDB (« Compact Disc DataBase » - base de données de disques audionumériques) permet à un utilisateur mal intentionné d'exécuter du code arbitraire.

4 Description

La bibliothèque *xine-lib* fournit un ensemble de fonctions permettant de construire un lecteur multimedia. Parmi les produits pouvant employer cette bibliothèque on trouve *xine*, *gxine*, les composants du bureau KDE *kdemultimedia* et *kaffeine*, du bureau Gnome *totem*,...

CDDB permet d'obtenir automatiquement l'artiste ou le groupe, le titre des morceaux lors de la lecture d'un disque audionumérique. Un bogue de format texte dans la gestion de la réponse du serveur peut être exploité pour exécuter du code arbitraire. En l'absence de problèmes sur les serveurs CDDB habituellement configurés, il faut donc préalablement qu'un agresseur parvienne à convaincre sa victime d'interroger un serveur sous son contrôle ou soit en mesure d'intercepter son traffic réseau.

5 Contournement provisoire

Supprimer la bibliothèque partagée *xineplug_inp_cdda.so* dans le répertoire des greffons de *xine-lib* (cependant la capacité à lire les disques audionumériques sera perdue).

6 Solution

Mettre à jour les sources en version 1.0.3 ou se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site de *Xine* :
  http://xinehq.de/
- Bulletin de sécurité Xine XSA-2005-1 :
  http://xinehq.de/index.php/security/XSA-2005-1
- Bulletin de sécurité Gentoo GLSA 200510-08 du 08 octobre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200510-08.xml
- Bulletin de sécurité Debian DSA 863-1 du 12 octobre 2005 :
  http://www.debian.org/security/2005/dsa-863
- Bulletin de sécurité Mandriva MDKSA-2005:180 du 12 octobre 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:180
- Référence CVE CAN-2005-2967 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2967

Gestion détaillée du document

10 octobre 2005 version initiale.

12 octobre 2005 ajout de la référence au bulletin de sécurité Debian DSA-863-1.