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 février 2005
N° CERTA-2004-AVI-257-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de SoX

Gestion du document

Référence	CERTA-2004-AVI-257-005
Titre	Vulnérabilité de SoX
Date de la première version	29 juillet 2004
Date de la dernière version	22 février 2005
Source(s)	Bulletin de sécurité Mandrake MDKSA-2004:076
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

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

SoX versions 12.17.2, 12.17.3 et 12.17.4.

3 Résumé

Deux vulnérabilités dans SoX permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire.

4 Description

SoX (Sound eXchange) est un utilitaire UNIX permettant de jouer, enregistrer et traduire des échantillons sonores dans différents formats.
Deux débordements de mémoire dans SoX permettent à un utilisateur mal intentionné, via la construction d'un

fichier musical d'extension `.wav`, de réaliser un déni de service ou d'exécuter du code arbitraire sur la plate-forme vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de `SoX` :
  http://sox.sourceforge.net
- Bulletin de sécurité Mandrake MDKSA-2004:076 du 28 juillet 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:076
- Bulletin de sécurité RedHat RHSA-2004:409 du 29 juillet 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-409.html
- Bulletin de sécurité Gentoo GLSA 200407-23 du 30 juillet 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200407-23.xml
- Bulletin de sécurité Debian DSA-565 du 13 octobre 2004 :
  http://www.debian.org/security/2004/dsa-565
- Bulletin de sécurité Fedora FLSA:1945 du 20 février 2005 :
  https://bugzilla.fedora.us/show_bug.cgi?id=1945
- Bulletin de sécurité OpenBSD pour sox du 31 juillet 2004 :
  http://www.vuxml.org/openbsd
- Bulletin de sécurité FreeBSD pour sox du 26 août 2004 :
  http://www.vuxml.org/freebsd
- Référence CVE CAN-2004-0557 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0557

Gestion détaillée du document

29 juillet 2004 version initiale.
30 juillet 2004 ajout de la référence au bulletin de sécurité RedHat.
02 août 2004 ajout des références aux bulletins de sécurité Gentoo et OpenBSD.
30 août 2004 ajout de la référence au bulletin de sécurité FreeBSD.
15 octobre 2004 ajout de la référence au bulletin de sécurité Debian.
22 février 2005 ajout de la référence au bulletin de sécurité Fedora.