Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 août 2006
N° CERTA-2006-AVI-299-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans libVNCServer

Gestion du document

Référence	CERTA-2006-AVI-299-002
Titre	Vulnérabilité dans libVNCServer
Date de la première version	18 juillet 2006
Date de la dernière version	08 août 2006
Source(s)	Rapport d'erreur Debian #376824
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

Contournement de la politique de sécurité.

2 Systèmes affectés

libVNCServer versions 0.8.1 et antérieures.

3 Résumé

Une vulnérabilité dans libVNCServer permet à un utilisateur distant de contourner la politique de sécurité du logiciel vulnérable.

4 Description

la bibliothèque de fonctions `libVNCServer` permet de mettre en œuvre des services de bureau distant comme par exemple `VNCServer`.
Une erreur présente dans les fonctions d'authentification de cette bibliothèque permet à un utilisateur distant de contourner l'authentification mise en place dans une application basée sur cette bibliothèque. Il peut alors obtenir un accès illégitime à tout ou partie de l'application vulnérable.

5 Solution

La version 0.8.2 de libVNCServer corrige le problème :
http://www.sourceforge.net/project/showfiles.php?group_id=32584

6 Documentation

- Site de libVNCServer :
  http://libvncserver.sourceforge.net
- Bulletin de sécurité Gentoo GLSA 200608-05 du 04 août 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200608-05.xml
- Bulletin de sécurité Suse SUSE-SA:2006:042 du 26 juillet 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Jul/0008.html
- Rapport d'erreur Debian #376824 :
  http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=376824
- Référence CVE CVE-2006-2450 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2450
- Bulletin de sécurité Gentoo GLSA 200608-12 du 07 août 2006 concernant x11vnc :
  http://www.gentoo.org/security/en/glsa/glsa-200608-12.xml

Gestion détaillée du document

18 juillet 2006 version initiale.
04 août 2006 ajout des références aux bulletins de sécurité Gentoo et Suse.
08 août 2006 ajout de la référence au bulletin de sécurité Gentoo concernant x11vnc.