Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 avril 2006
N° CERTA-2006-AVI-130-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Dia

Gestion du document

Référence	CERTA-2006-AVI-130-003
Titre	Vulnérabilités de Dia
Date de la première version	31 mars 2006
Date de la dernière version	24 avril 2006
Source(s)	Site du projet
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

Les versions de Dia comprises entre 0.87 et 0.94, ainsi que les versions de test 0.95 1 à 5.

3 Résumé

Plusieurs vulnérabilités dans Dia permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Dia est un outil de création de schémas vectoriels fonctionnant sur la plupart des systèmes d'exploitation. Plusieurs dépassements de mémoire sont possibles lorsque des fichiers de type `XFig` sont ouverts. Un utilisateur malveillant peut profiter de ces vulnérabilités pour exécuter du code arbitraire sur le système où Dia a été exécuté.

5 Solution

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

6 Documentation

- Site du projet Dia :
  http://www.gnome.org/projects/dia/
- Bulletin de sécurité Ubuntu USN-266 du 3 avril 2006 :
  http://www.ubuntu.com/usn/usn-266-1
- Bulletin de sécurité Mandriva MDKSA-2006:062 du 3 avril 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:062
- Bulletin de sécurité Debian DSA-1025 du 6 avril 2006 :
  http://www.debian.org/security/2006/dsa-1025
- Bulletin de sécurité Gentoo GLSA 200604-14 du 23 avril 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200604-14.xml
- Mise à jour de sécurité Fedora pour Dia :
  http://download.fedora.redhat.com/pub/fedora/linux/updates/4/
- Référence CVE CVE-2006-1550 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1550

Gestion détaillée du document

31 mars 2006 version initiale.
04 avril 2006 ajout des références aux bulletins de sécurité Ubuntu et Mandriva.
06 avril 2006 ajout des références aux bulletins de sécurité Debian et Fedora.
24 avril 2006 ajout de la référence au bulletin de sécurité Gentoo.