

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Dia

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-2006-AVI-211>

Gestion du document

Référence	CERTA-2006-AVI-211-003
Titre	Vulnérabilité de Dia
Date de la première version	23 mai 2006
Date de la dernière version	08 juin 2006
Source(s)	Mise à jour du projet Dia
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

La version Dia 0.95 et celles antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans Dia. Elle peut permettre à un utilisateur malveillant d'exécuter des commandes arbitraires à distance.

4 Description

Une vulnérabilité de type débordement de mémoire a été identifiée dans l'éditeur graphique Dia. La gestion des noms de fichiers n'est pas correctement effectuée par la fonction `gtk_message_dialog_new()`. Une personne malveillante peut faire parvenir un fichier au nom singulier. Si l'utilisateur l'ouvre par la fenêtre Dia standard ("Open Diagram"), des commandes arbitraires peuvent s'exécuter à son insu.

5 Solution

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

6 Documentation

- Site Internet du projet Dia :
<http://www.gnome.org/projects/dia/>
- Correctif fourni par Gnome Bugzilla :
<http://bugzilla.gnome.org/attachment.cgi?id=65665&action=view>
- Bulletin de sécurité Mandriva MDKSA-2006:093 du 30 mai 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:093>
- Bulletin de sécurité Ubuntu USN-286-1 du 24 mai 2006 :
<http://www.ubuntu.com/usn/usn-286-1>
- Bulletin de sécurité RedHat RHSA-2006:0541 du 01 juin 2006 :
<https://rhn.redhat.com/errata/RHSA-2006-0541.html>
- Bulletin de sécurité Gentoo GLSA 200606-03 du 07 juin 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200606-03.xml>
- Référence CVE CVE-2006-2453 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2453>
- Référence CVE CVE-2006-2480 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2480>

Gestion détaillée du document

23 mai 2006 version initiale.

01 juin 2006 ajout des références aux bulletins de sécurité Mandriva et Ubuntu.

07 juin 2006 ajout de la référence CVE CVE-2006-2453 et du bulletin de sécurité RedHat.

08 juin 2006 ajout de la référence au bulletin de sécurité Gentoo.