



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2005
N° CERTA-2005-AVI-387

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2005-AVI-387>

Gestion du document

Référence	CERTA-2005-AVI-387
Titre	Vulnérabilité dans Dia
Date de la première version	10 octobre 2005
Date de la dernière version	-
Source(s)	Bulletin de sécurité Ubuntu USN-193-1 du 04 octobre 2005
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

Dia versions 0.94 et antérieures.

3 Résumé

Une vulnérabilité dans Dia permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Dia est un outil de création de schémas vectoriels. Il dispose d'un module développé en Python mettant en œuvre le support des fichiers de type SVG (Scalable Vector Graphics). Un manque de contrôle des données fournies à ce module permet à un utilisateur distant mal intentionné d'exécuter du script arbitraire en Python par le biais d'un fichier SVG malicieusement construit.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention de correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA-847 du 08 octobre 2005 :
<http://www.debian.org/security/2005/dsa-847>
- Bulletin de sécurité Ubuntu USN-193-1 du 04 octobre 2005 :
<http://www.ubuntu.com/usn/usn-193-1>
- Référence CVE : CAN-2005-2966
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2966>

Gestion détaillée du document

10 octobre 2005 version initiale.