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 février 2006
N° CERTA-2005-AVI-221-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de gedit

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-221

Gestion du document

Référence	CERTA-2005-AVI-221-003
Titre	Vulnérabilité de gedit
Date de la première version	16 juin 2005
Date de la dernière version	24 février 2006
Source(s)	Bulletin de sécurité Gentoo GLSA 200506-09 du 11 juin 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.

2 Systèmes affectés

Toutes les versions de gedit antérieures à la version 2.10.3.

3 Description

Une vulnérabilité de type débordement de mémoire dans gedit permet à un utilisateur mal intentionné, via un fichier dont le nom est habilement constitué, d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Solution

Mettre à jour gedit en version 2.10.3.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet de gedit :
  http://www.gnome.org/projects/gedit/
- Bulletin de sécurité Gentoo GLSA 200506-09 du 11 juin 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200506-09.xml
- Bulletin de sécurité RedHat RHSA-2005:499 du 13 juin 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-499.html
- Bulletin de sécurité Mandriva MDKSA-2005:102 du 15 juin 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:102
- Mise à jour de sécurité Fedora Core 3 pour gedit du 27 juin 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
- Mise à jour de sécurité Fedora Core 2 pour gedit du 27 juin 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
- Bulletin de sécurité Debian DSA-753 du 12 juillet 2005 :
  http://www.debian.org/security/2005/dsa-753
- Bulletin de sécurité FreeBSD du 20 février 2006 :
  http://www.vuxml.org/freebsd/pkg-gedit.html
- Référence CVE CAN-2005-1686 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1686

Gestion détaillée du document

16 juin 2005 version initiale.
27 juin 2005 ajout des références aux mises à jour de sécurité Fedora.
12 juillet 2005 ajout de la référence au bulletin de sécurité Debian.
24 février 2006 ajout de la référence au bulletin de sécurité FreeBSD.