



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 décembre 2006
N° CERTA-2006-AVI-523

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel GnuPG

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-523>

Gestion du document

Référence	CERTA-2006-AVI-523
Titre	Vulnérabilité du logiciel GnuPG
Date de la première version	04 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité GnuPG
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

GnuPG versions 1.4 et 2.0.

3 Résumé

Une vulnérabilité a été découverte dans GnuPG. Cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

GnuPG est un outil de chiffrement sous licence GNU.

Une vulnérabilité a été découverte dans GnuPG. Cette vulnérabilité, résultant d'une erreur aux limites dans la fonction `ask_outfile_name()`, peut être exploitée par un attaquant afin d'exécuter du code arbitraire sur la machine cible.

Cette vulnérabilité n'est exploitable que si le *mode interactif* est utilisé.

5 Solution

Appliquer le correctif fourni par l'éditeur (cf. Documentation).

6 Documentation

- Bulletin de sécurité GnuPG :
<http://lists.gnupg.org/pipermail/gnupg-announce/2006q4/000241.html>
- Correctif de l'éditeur:
<http://cvs.gnupg.org/cgi-bin/viewcvs.cgi/branches/STABLE-BRANCH-1-4/g10/openfile.c?rev=4349&r1=4215&r2=4349>
- Référence CVE CVE-2006-6169 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6169>

Gestion détaillée du document

04 décembre 2006 version initiale.