



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 mars 2006  
N° CERTA-2006-AVI-103-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-103>

---

### Gestion du document

Référence	CERTA-2006-AVI-103-002
Titre	Vulnérabilité dans GnuPG
Date de la première version	13 mars 2006
Date de la dernière version	16 mars 2006
Source(s)	Bulletin de sécurité GnuPG du 9 mars 2006
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

Atteinte à l'intégrité des données.

### 2 Systèmes affectés

GnuPG versions 1.4.2.1 et antérieures.

### 3 Résumé

Une vulnérabilité dans GnuPG permet à un utilisateur de porter atteinte à l'intégrité des données.

### 4 Description

GnuPG présente une erreur dans la mise en œuvre du contrôle de la validité d'une signature accompagnant un document. Elle permet à un utilisateur d'insérer des données arbitraires dans un document signé (typiquement du texte supplémentaire dans un message) sans que GnuPG détecte une erreur d'intégrité.

## 5 Solution

La version 1.4.2.2 de GnuPG corrige le problème :  
<http://www.gnupg.org/download/>

## 6 Documentation

- Site de GnuPG :  
<http://www.gnupg.org>
- Bulletin de sécurité GnuPG du 9 mars 2006 :  
<http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000216.html>
- Bulletin de sécurité Debian DSA 993 du 10 mars 2006 :  
<http://www.debian.org/security/2006/dsa-993>
- Bulletin de sécurité FreeBSD pour GnuPG du 10 mars 2006 :  
<http://www.vuxml.org/freebsd/pkg-gnupg.html>
- Bulletin de sécurité Gentoo GLSA 200603-08 du 10 mars 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200603-08.xml>
- Bulletin de sécurité Ubuntu USN-264-1 du 13 mars 2006 :  
<http://www.ubuntulinux.org/usn/usn-264-1>
- Bulletin de sécurité Mandriva MDKSA-2006:055 du 13 mars 2006 :  
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:055>
- Bulletin de sécurité RedHat RHSA-2006:0266 du 15 mars 2006 :  
<https://rhn.redhat.com/errata/RHSA-2006-0266.html>
- Référence CVE CVE-2006-0049 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0049>

## Gestion détaillée du document

**13 mars 2006** version initiale.

**14 mars 2006** ajout des références aux bulletins de sécurité Gentoo et Mandriva, corrections références Debian et FreeBSD.

**16 mars 2006** ajout de la référence au bulletin de sécurité RedHat.