

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-086>

---

### Gestion du document

Référence	CERTA-2006-AVI-086-002
Titre	Vulnérabilité de GnuPG
Date de la première version	21 février 2006
Date de la dernière version	02 mars 2006
Source(s)	Bulletin de sécurité Debian DSA-978 du 17 février 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

Toutes les versions GnuPG antérieures à la version 1.4.2.1.

## 3 Description

GnuPG (GNU Privacy Guard) est un logiciel libre remplaçant de PGP (Pretty Good Privacy). Une vulnérabilité dans GnuPG permet à un utilisateur mal intentionné de contourner la vérification de signature en utilisant une erreur de programmation de type faux positif. Cette erreur concerne l'outil `gpgv` et la commande `gpg -verify`.

## 4 Solution

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

## 5 Documentation

- Site Internet de GnuPG :  
<http://www.gnupg.org>
- Bulletin de sécurité Debian DSA 978 du 17 février 2006 :  
<http://www.debian.org/security/2006/dsa-978>
- Bulletin de sécurité Gentoo GLSA-200602-10 du 18 février 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200602-10.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:043 du 17 février 2006 :  
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:043>
- Bulletin de sécurité Ubuntu USN-252-1 du 17 février 2006 :  
<http://www.ubuntulinux.org/usn/usn-252-1>
- Bulletin de sécurité du port FreeBSD de GnuPG du 17 février 2006 :  
<http://www.vuxml.org/freebsd/pkg-gnupg.html>
- Bulletin de sécurité SUSE SUSE-SA:2006:009 du 20 février 2006 :  
[http://www.novell.com/linux/security/advisories/2006\\_09\\_gpg.html](http://www.novell.com/linux/security/advisories/2006_09_gpg.html)
- Bulletin de sécurité SUSE SUSE-SA:2006:013 du 02 mars 2006 :  
[http://www.novell.com/linux/security/advisories/2006\\_13\\_gpg.html](http://www.novell.com/linux/security/advisories/2006_13_gpg.html)
- Référence CVE CVE-2006-0455 :  
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2006-0455>

### Gestion détaillée du document

**21 février 2006** version initiale.

**27 février 2006** ajout de la référence au bulletin de sécurité SUSE SUSE-SA:2006:009.

**02 mars 2006** ajout de la référence au bulletin de sécurité SUSE SUSE-SA:2006:013.