

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-2007-AVI-114>

Gestion du document

Référence	CERTA-2007-AVI-114-002
Titre	Vulnérabilité dans GnuPG
Date de la première version	09 mars 2007
Date de la dernière version	26 mars 2007
Source(s)	Bulletin de sécurité SecurityFocus du 05 mars 2007
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

GnuPG versions 1.4.6 et antérieures.

3 Résumé

Une vulnérabilité dans GnuPG permet à un utilisateur malintentionné de contourner la politique de sécurité du logiciel.

4 Description

Lors de l'affichage de messages contenant plusieurs parties, le logiciel GnuPG ne permet pas de distinguer les parties signées de celles qui ne le sont pas. Il est donc possible pour un utilisateur mal intentionné d'insérer dans un message partiellement signé du contenu non-vérifiable.

5 Solution

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

6 Documentation

- Bulletin de sécurité SecurityFocus du 05 mars 2007 :
<http://www.securityfocus.com/bid/22757>
- Bulletin de sécurité Debian DSA-1266 du 13 mars 2007 :
<http://www.debian.com/security/2007/dsa-1266>
- Bulletin de sécurité Mandriva MDKSA-2007:059 du 08 mars 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:059>
- Bulletin de sécurité Ubuntu USN-432-1 du 08 mars 2007 :
<http://www.ubuntulinux.org/usn/usn-432-1>
- Bulletin de sécurité Ubuntu USN-432-2 du 13 mars 2007 :
<http://www.ubuntulinux.org/usn/usn-432-2>
- Bulletin de sécurité Fedora 6 Fedora-2007-315 du 12 mars 2007 :
<http://fedoranews.org/cms/node/2774>
- Bulletin de sécurité Fedora 5 Fedora-2007-316 du 12 mars 2007 :
<http://fedoranews.org/cms/node/2775>
- Bulletin de sécurité Red Hat RHSA-2007:0106-2 du 06 mars 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0106.html>
- Référence CVE CVE-2007-1263 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1263>

Gestion détaillée du document

09 mars 2007 version initiale.

13 mars 2007 ajout des références aux bulletins de sécurité Fedora et Red Hat.

26 mars 2007 ajout des références aux bulletins de sécurité Ubuntu et Debian.