

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-2008-AVI-172>

Gestion du document

Référence	CERTA-2008-AVI-172
Titre	Vulnérabilité du logiciel GnuPG
Date de la première version	02 avril 2008
Date de la dernière version	–
Source(s)	Avis de mise à jour GnuPG du 26 mars 2008
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 ;
- déni de service à distance.

2 Systèmes affectés

- GnuPG / gpg versions antérieures à la version 1.4.9 ;
- GnuPG / gpg versions antérieures à la version 2.0.9.

3 Résumé

Une vulnérabilité a été découverte dans le logiciel GnuPG. Cette vulnérabilité peut être exploitée à distance afin de réaliser un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité a été découverte dans le logiciel GnuPG. Cette vulnérabilité due à une erreur dans la gestion de clés, lorsque celles-ci disposent de numéros d'identification dupliqués, provoquant une corruption de la mémoire.

Cette vulnérabilité peut être exploitée par un utilisateur malintentionné afin de réaliser un déni de service, ou d'exécuter du code arbitraire, à partir de la machine, ou via un serveur de clefs distant.

5 Solution

Mettre à jour vers les versions 1.4.8 ou 2.0.8 (cf. Documentation).

6 Documentation

- Annonce de mise à jour GnuPG du 26 mars 2008 :
<http://lists.gnupg.org/pipermail/gnupg-announce/2008q1/000272.html>
<ftp://ftp.gnupg.org/gcrypt/gnupg>
- Bulletin de sécurité de l'ocCERT numéro 2008-01 :
<http://www.ocert.org/advisories/ocert-2008-1.html>
- Référence CVE CVE-2008-1530 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1530>

Gestion détaillée du document

02 avril 2008 version initiale.