

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-267>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2006-AVI-267-003 |
| Titre | Vulnérabilité dans GnuPG |
| Date de la première version | 29 juin 2006 |
| Date de la dernière version | 04 août 2006 |
| Source(s) | Liste des changements apportés à la version 1.4.4 de GnuPG du 25 juin 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

- Exécution de code arbitraire ;
- déni de service local ou distant.

2 Systèmes affectés

- GnuPG versions 1.4.3 et antérieures ;
- GnuPG versions 1.9.20 et antérieures.

3 Résumé

Une vulnérabilité dans GnuPG permet à un utilisateur local de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Un manque de contrôle dans la taille du champ `user ID` d'un message GPG dans GnuPG permet à un utilisateur de provoquer un déni de service de l'application ou d'exécuter du code arbitraire par le biais d'un message

construit de façon particulière. Cette action malveillante peut se faire localement, ou à distance, par le biais d'une application tierce comme un client de messagerie.

5 Solution

Les versions 1.4.4 (stable) et 1.9.21 (développement) de GnuPG corrigent le problème :

<http://www.gnupg.org/download>

6 Documentation

- Liste des changements apportés à la version 1.4.4 de GnuPG :
<http://lists.gnupg.org/pipermail/gnupg-announce/2006q2/000226.html>
- Bulletin de sécurité Mandriva MDKSA-2006:110 du 29 juin 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:110>
- Bulletin de sécurité Debian DSA-1107 du 10 juillet 2006 :
<http://www.debian.org/security/2006/DSA-1107>
- Bulletin de sécurité Debian DSA-1115 du 21 juillet 2006 :
<http://www.debian.org/security/2006/DSA-1115>
- Bulletin de sécurité RedHat RHSA-2006:0571 du 18 juillet 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0571>
- Bulletin de sécurité SGI 20060701-01-U du 20 juillet 2006 :
<ftp://patches.sgi.com/support/free/security/advisories/20060701-01-U.asc>
- Bulletin de sécurité Suse SUSE-SR:2006:015 du 30 juin 2006 :
http://www.novell.com/linux/security/advisories/2006_38_security.html
- Bulletin de sécurité Ubuntu USN-304-1 du 26 juin 2006 :
<http://www.ubuntu.com/usn/usn-304-1>
- Référence CVE CVE-2006-3082 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3082>

Gestion détaillée du document

29 juin 2006 version initiale ;

6 juillet 2006 précision sur les risques associés ;

24 juillet 2006 ajout des références au bulletins de sécurité Debian.

04 août 2006 ajout des références au bulletins de sécurité RedHat, SGI, Suse et Ubuntu.