

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de kppp

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-2005-AVI-098>

Gestion du document

| | |
|-----------------------------|-----------------------------|
| Référence | CERTA-2005-AVI-098-002 |
| Titre | Vulnérabilité de kppp |
| Date de la première version | 03 mars 2005 |
| Date de la dernière version | 09 mars 2005 |
| Source(s) | Bulletin de sécurité de kde |
| 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 ;
- usurpation d'identité.

2 Systèmes affectés

KDE 3.1.5 et versions antérieures.

3 Description

Kppp est une application graphique de l'environnement KDE qui permet l'établissement de connexions ppp.

Une vulnérabilité présente dans kppp peut être exploitée par un utilisateur local mal intentionné afin de modifier le contenu des fichiers `/etc/hosts` et `/etc/resolv.conf` utilisés pour la résolution de noms (association adresse IP-nom de machine).

4 Contournement provisoire

Dans l'attente de l'application du correctif, supprimer le drapeau `suid` sur le fichier `/usr/sbin/kppp`.

5 Solution

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

6 Documentation

- Bulletin de sécurité KDE du 28 février 2005 :
<http://www.kde.org/info/security/advisory-20050228-1.txt>
- Bulletin de sécurité iDefense du 28 février 2005 :
<http://www.iddefense.com/application/poi/display?id=208&type=vulnerabilities>
- Bulletin de sécurité RedHat RHSA-2005:175 du 03 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-175.html>
- Bulletin de sécurité Debian DSA-692 du 08 mars 2005 :
<http://www.debian.org/security/2005/dsa-692>
- Mise à jour de sécurité du paquetage NetBSD kdenetwork3 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/kdenetwork3/README.html>
- Référence CVE CAN-2005-0205 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0205>

03 mars 2005 version initiale.

07 mars 2005 ajout de la référence au bulletin de sécurité RedHat.

09 mars 2005 ajout des références aux bulletins de sécurité Debian et NetBSD.