



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 04 février 2005
N° CERTA-2005-AVI-040-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ncpfs

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-040>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2005-AVI-040-002 |
| Titre | Vulnérabilité de ncpfs |
| Date de la première version | 31 janvier 2005 |
| Date de la dernière version | 04 février 2005 |
| Source(s) | Bulletin de sécurité Gentoo GLSA 200501-44 |
| 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

- Elévation de privilèges ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

ncpfs pour GNU/Linux, versions 2.2.5 et versions antérieures.

3 Résumé

Deux vulnérabilités dans ncpfs permettent à un utilisateur mal intentionné d'élever ses privilèges ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

ncpfs est un pilote pour le système de fichiers réseau supportant le protocole NCP (NetWare Core Protocol). Une vulnérabilité de type débordement de mémoire présente dans le programme ncplogin permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur la plate-forme vulnérable (CVE CAN-2005-0014).

Une seconde vulnérabilité dans le fichier source `nwclient.c` permet à un utilisateur mal intentionné d'élever ses privilèges (CVE CAN-2005-0013).

5 Solution

Mettre à jour `nepfs` en version 2.2.6 ou toute version supérieure.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de `nepfs` :
<ftp://platan.vc.cvut.cz/pub/linux/nepfs/>
- Liste des changements dans la version 2.2.6 de `nepfs` :
<ftp://platan.vc.cvut.cz/pub/linux/nepfs/Changes-2.2.6>
- Bulletin de sécurité Gentoo GLSA 200501-44 du 30 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-44.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:028 du 01 février 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:028>
- Bulletin de sécurité Debian DSA-665 du 04 février 2005 :
<http://www.debian.org/security/2005/dsa-665>
- Référence CVE CAN-2005-0013 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0013>
- Référence CVE CAN-2005-0014 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0014>

Gestion détaillée du document

31 janvier 2005 version initiale.

02 février 2005 ajout de la référence au bulletin de sécurité Mandrake MDKSA-2005:028.

04 février 2005 ajout de la référence au bulletin de sécurité Debian DSA-665.