Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 avril 2005
N° CERTA-2005-AVI-132

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de portupgrade

Gestion du document

Référence	CERTA-2005-AVI-132
Titre	Vulnérabilité de portupgrade
Date de la première version	12 avril 2005
Date de la dernière version	–
Source(s)	CVE : CAN-2005-0610 Avis FreeBSD : VuXML
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 ;
- élévation de privilège ;
- d'un utilisateur local.

2 Systèmes affectés

Les versions du logiciel `portupgrade` strictement inférieures à 20041226_2.

3 Description

`portupgrade` est un logiciel destiné à mettre à jour les logiciels installés sur un système d'exploitation FreeBSD.

Une vulnérabilité liée à la gestion des fichiers temporaires permet à un utilisateur local malicieux de :

- écraser n'importe quel fichier ;
- d'exécuter n'importe quelle commande avec les droits du superutilisateur ;

4 Contournement provisoire

Placer la variable d'environnement `PKG_TMPDIR` avec le nom d'un réperrtoire dans lequel seul l'utilisateur qui exécute `portupgrade` peut écrire.

5 Solution

Mettre à jour `portupgrade`.

6 Documentation

- Référence CVE : CAN-2005-0610
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0610 ;
- FreeBSD, bulletin de sécurité du 2005-04-12 :
  http://www.vuxml.org/freebsd/pkg-portupgrade.html

Gestion détaillée du document

12 avril 2005 version initiale.