Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 juillet 2004
N° CERTA-2004-AVI-216-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de pavuk

Gestion du document

Référence	CERTA-2004-AVI-216-002
Titre	Vulnérabilité de pavuk
Date de la première version	01 juillet 2004
Date de la dernière version	05 juillet 2004
Source(s)	Bulletin de sécurité Gentoo GLSA 200406-22
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.

2 Systèmes affectés

`pavuk` version 0.9p128 et versions antérieures.

3 Résumé

Une vulnérabilité dans l'outil `pavuk` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`pavuk` est un programme de récupération récursif de documents supportant les protocoles HTTP, FTP et Gopher.
Lorsqu'un serveur HTTP renvoi un code d'erreur 305 (`Use Proxy`), `pavuk` copie les données contenues dans l'en-tête `HTTP Location` d'une manière non sécurisée. Cela permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les droits de l'utilisateur ayant exécuté `pavuk`.

5 Solution

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

6 Documentation

- Site Internet de `pavuk` :
  http://www.idata.sk/~ondrej/pavuk/
- Bulletin de sécurité Gentoo GLSA 200406-22 du 30 juin 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200406-22.xml
- Bulletin de sécurité Debian DSA-527 du 03 juillet 2004 :
  http://www.debian.org/security/2004/dsa-527
- Bulletin de sécurité FreeBSD pour pavuk du 03 juillet 2004 :
  http://www.vuxml.org/freebsd/
- Référence CVE CAN-2004-0456 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0456

Gestion détaillée du document

01 juillet 2004 version initiale.
02 juillet 2004 ajout de la référence CVE et de la version impactée.
05 juillet 2004 ajout des références aux bulletins de sécurité Debian et FreeBSD.