



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 janvier 2005
N° CERTA-2004-AVI-255-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Pavuk

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-2004-AVI-255>

Gestion du document

Référence	CERTA-2004-AVI-255-001
Titre	Vulnérabilité de Pavuk
Date de la première version	28 juillet 2004
Date de la dernière version	17 janvier 2005
Source(s)	Bulletin de sécurité GLSA 200407-19 de Gentoo
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 Description

pavuk est un outil permettant d'aspirer les sites web.

Une vulnérabilité de type débordement de mémoire est présente dans la routine de traitement des données d'authentification renvoyées par le serveur web (erreur HTTP 401).

En mettant à disposition un site habilement constitué, il est ainsi possible de forcer l'exécution de code arbitraire à distance sur une plate-forme utilisant une version vulnérable de pavuk.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

5 Documentation

- Site Internet de pavuk :
<http://www.idata.sk/~ondrej/pavuk/>
- Bulletin de sécurité Gentoo GLSA 200407-19 du 26 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-19.xml>
- Bulletin de sécurité Avaya ASA-2005-006 :
http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549RHSA-2004-505RHSA-2004-689.pdf

Gestion détaillée du document

28 juillet 2004 version initiale.

17 janvier 2005 ajout référence au bulletin de sécurité Avaya ASA-2005-006.