



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 mai 2008
N° CERTA-2008-AVI-238

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans CUPS

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-2008-AVI-238>

Gestion du document

Référence	CERTA-2008-AVI-238
Titre	Vulnérabilité dans CUPS
Date de la première version	13 mai 2008
Date de la dernière version	–
Source(s)	Suivi des bogues #2790 de CUPS
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

CUPS versions 1.3.7 et antérieures.

3 Résumé

Une vulnérabilité dans le traitement des images au format PNG dans CUPS permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité a été découverte dans le traitement des images au format PNG par le gestionnaire d'impression CUPS. Un utilisateur malintentionné peut, par le biais d'une image ayant de très grandes dimensions, provoquer l'exécution de code arbitraire à distance.

5 Solution

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

6 Documentation

- Suivi des bogues #2790 de CUPS :
<http://www.cups.org/str.php?L2790>
- Téléchargement de CUPS :
<http://www.cups.org/software.php>
- Mise à jour de sécurité Fedora 7 du 10 mai 2008 :
<http://www.redhat.com/archives/fedora-package-announce/2008-May/msg00081.html>
- Mise à jour de sécurité Fedora 8 du 10 mai 2008 :
<http://www.redhat.com/archives/fedora-package-announce/2008-May/msg00068.html>
- Bulletin de sécurité Gentoo GLSA-200804-23 du 18 avril 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200804-23.xml>
- Bulletin de sécurité Ubuntu USN-606-1 du 05 mai 2008 :
<http://www.ubuntu.com/usn/usn-606-1>
- Référence CVE CVE-2008-1722 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1722>

Gestion détaillée du document

13 mai 2008 version initiale.