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 avril 2008
N° CERTA-2008-AVI-183

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans CUPS

Gestion du document

Référence	CERTA-2008-AVI-183
Titre	Vulnérabilités dans CUPS
Date de la première version	04 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de mise à jour CUPS 1.3.7 du 01 avril 2008
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 1.3.6 et antérieures.

3 Résumé

Deux vulnérabilités permettant l'exécution de code arbitraire à distance ont été découvertes dans *CUPS*.

4 Description

Deux vulnérabilités ont été découvertes dans *CUPS* :

– un débordement de mémoire dans le script `cgiCompileSearch` permet l'exécution de code arbitraire à distance (CVE-2008-0047) ;
– un débordement de mémoire dans le filtre de traitement des images au format `GIF` permet également l'exécution de code arbitraire à distance (CVE-2008-1373).

5 Solution

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

6 Documentation

- Bulletin de mise à jour CUPS 1.3.7 du 01 avril 2008 :
  http://www.cups.org/articles.php?L537
- Bulletin de sécurité Gentoo GLSA-200804-01 du 01 avril 2008 :
  http://www.gentoo.org/security/en/glsa/glsa-200804-01.xml
- Bulletin de sécurité RedHat RHSA-2008:0206 du 01 avril 2008 :
  http://rhn.redhat.com/errata/RHSA-2008-0206.html
- Bulletin de sécurité Ubuntu USN-598-1 du 02 avril 2008 :
  http://www.ubuntulinux.org/usn/usn-598-1
- Référence CVE CVE-2008-0047 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0047
- Référence CVE CVE-2008-1373 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1373

Gestion détaillée du document

04 avril 2008 version initiale.