



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 novembre 2007
N° CERTA-2007-AVI-467-002

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-2007-AVI-467>

Gestion du document

Référence	CERTA-2007-AVI-467-002
Titre	Vulnérabilité dans CUPS
Date de la première version	02 novembre 2007
Date de la dernière version	06 novembre 2007
Source(s)	Bulletin de sécurité CUPS du 31 octobre 2007
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 ;
- déni de service à distance.

2 Systèmes affectés

CUPS 1.x.

3 Résumé

Une vulnérabilité dans CUPS permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une erreur a été identifiée dans le serveur d'impression CUPS. Elle est relative à la fonction *IppReadIO()* intervenant dans la mise en œuvre du protocole IPP (Internet Printing Protocol). Cette vulnérabilité de type débordement de mémoire permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire par le biais d'une requête IPP construite de façon particulière.

5 Solution

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

6 Documentation

- Site de CUPS :
<http://www.cups.org>
- Bulletin de sécurité de CUPS du 31 octobre 2007 :
<http://www.cups.org/str.php?L2561>
- Bulletin de sécurité de Mandriva MDKSA-2007:204 du 01 novembre 2007 :
<http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:204>
- Bulletin de sécurité de SuSE SUSE-SA:2007:058 du 31 octobre 2007 :
<http://lists.opensuse.org/opensuse-security-announce/2007-10/msg00010.html>
- Bulletin de sécurité de Red Hat RHSA-2007:1020 du 31 octobre 2007 :
<http://www.rhn.redhat.com/errata/RHSA-2007-1020.html>
- Bulletin de sécurité de Ubuntu USN-539-1 du 06 novembre 2007 :
<http://www.ubuntu.com/usn/usn-539-1>
- Note de vulnérabilité de l'US-CERT VU#446897 du 01 novembre 2007 :
<http://www.kb.cert.org/vuls/id/446897>
- Référence CVE CVE-2007-4351 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4351>

Gestion détaillée du document

02 novembre 2007 version initiale.

05 novembre 2007 ajout des références aux bulletins de sécurité Mandriva, SuSE et Red Hat.

06 novembre 2007 ajout de la référence au bulletin de sécurité Ubuntu.