

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-156>

Gestion du document

Référence	CERTA-2008-AVI-156-001
Titre	Vulnérabilité dans CUPS
Date de la première version	20 mars 2008
Date de la dernière version	27 mars 2008
Source(s)	Bulletin de mise à jour CUPS 1.3.6 du 19 février 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 ;
- déni de service à distance.

2 Systèmes affectés

Les versions de CUPS antérieures à 1.3.6.

3 Résumé

Le logiciel CUPS (*Common UNIX Printing System*) est vulnérable via son service de partage d'imprimante.

4 Description

Le service de CUPS permettant de partager une imprimante, tournant sur le port 631/TCP, est vulnérable à des attaques de type débordement de mémoire. Une personne malveillante peut, à distance, à l'aide d'un paquet spécifiquement réalisé, provoquer un déni de service ou exécuter du code arbitraire.

5 Solution

Se référer au bulletin de mise à jour de CUPS 1.3.6 du 19 février 2008 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de mise à jour de CUPS 1.3.6 du 19 février 2008 :
<http://www.cups.org/articles.php?L529>
- Bulletin de sécurité Apple 307562 du 18 mars 2008 :
<http://docs.info.apple.com/article.html?artnum=307562>
- Bulletin de sécurité SuSE SUSE-SA-2008-015 du 19 mars 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00005.html>
- Bulletin de sécurité SuSE SUSE-SA-2008-012 du 06 mars 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00005.html>
- Bulletin de sécurité Debian DSA-1530 du 25 mars 2008 :
<http://www.debian.org/security/2008/dsa-1530>
- Bulletin de sécurité Mandriva MDVSA-2008-051 du 26 février 2008 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:051>
- Bulletin de sécurité Mandriva MDVSA-2008-050 du 26 février 2008 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:050>
- Bulletin de sécurité Red Hat RHSA-2008:0157-5 du 21 février 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0157.html>
- Référence CVE CVE-2008-0047 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0047>
- Référence CVE CVE-2008-0882 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0882>

Gestion détaillée du document

20 mars 2008 version initiale.

27 mars 2008 ajout d'une référence CVE et de références aux bulletins de distributions Linux.