

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service d'impression 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-2003-AVI-094>

Gestion du document

Référence	CERTA-2003-AVI-094-002
Titre	Vulnérabilité du service d'impression CUPS
Date de la première version	30 mai 2003
Date de la dernière version	12 juin 2003
Source(s)	Bulletin de sécurité RHSA-2003:171 de Red Hat Bulletin de sécurité MDKSA-2003:062 de Mandrake
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

Déni de service.

2 Systèmes affectés

Toutes les versions de CUPS antérieures ou égales à la version 1.1.19rc3.

3 Résumé

Un déni de service est possible sur le serveur d'impression CUPS.

4 Description

CUPS (Common Unix Printing System) est un serveur d'impression basé sur IPP (Internet Printing Protocol).

Une vulnérabilité présente dans la gestion des requêtes IPP peut être exploitée par un utilisateur mal intentionné afin de bloquer tout accès au service d'impression.

5 Contournement provisoire

Filtrer l'accès au port 631/tcp utilisé par IPP afin de limiter l'exploitation de cette vulnérabilité.

6 Solution

Appliquer le correctif fourni par l'éditeur :

- Bulletin de sécurité MDKSA-2003:062 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:062>
- Bulletin de sécurité RHSA-2003:171 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-171.html>
- Bulletin de sécurité SuSE-SA:2003:028 de SuSE :
http://www.suse.com/de/security/2003_028.html
- Bulletin de sécurité DSA-317 de Debian :
<http://www.debian.org/security/2003/dsa-317>

7 Documentation

- Annonce "CUPS Denial of Service Attack Vulnerability" :
<http://www.cups.org/news.php?V119>
- Référence CVE CAN-2003-0195 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0195>

Gestion détaillée du document

30 mai 2003 version initiale.

10 juin 2003 Ajout référence au bulletin de sécurité de SuSE.

12 juin 2003 Ajout référence au bulletin de sécurité de debian.