

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2005-AVI-018>

Gestion du document

Référence	CERTA-2005-AVI-018-001
Titre	Multiples vulnérabilité dans CUPS
Date de la première version	19 janvier 2005
Date de la dernière version	17 février 2005
Source(s)	CVE : CAN-2004-1267 CVE : CAN-2004-1268 CVE : CAN-2004-1269 CVE : CAN-2005-1270
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

- intégrité et confidentialité des données ;
- déni de service sur la gestion des imprimantes ;

2 Systèmes affectés

Les versions de CUPS antérieures à la version 1.3.23.

3 Résumé

4 Description

CUPS est un logiciel qui fournit aux systèmes d'exploitation basés sur UNIX un système d'impression portable.

Plusieurs vulnérabilités ont été publiées sur CUPS :

CAN-2004-1267 HPGL est format de fichier contenant des graphiques vectoriels, tels que ceux produits par exemple par les systèmes de conception assistés par ordinateur à destination de certaines tables traçantes.

Le logiciel CUPS offre à ses utilisateurs la possibilité d'imprimer un fichier au format HPGL sur n'importe quelle imprimante gérée par CUPS, grâce à un programme appelé `hpgltops`.

`hpgltops` est vulnérable à un débordement de variable. Un utilisateur mal intentionné peut soumettre à l'impression un fichier au format HPGL astucieusement construit. Cela permet d'exécuter du code arbitraire avec les droits du gestionnaire d'impression (souvent c'est l'utilisateur « `lp` »). Un tel code en particulier pourrait en particulier lire ou modifier les documents en cours d'impression.

CAN-2004-1268

CAN-2004-1269 Le programme `lppasswd` fait partie du logiciel CUPS. Il permet de définir, de changer et de supprimer des mots de passe spécifiques pour la gestion des imprimantes. Une faille du programme `lppasswd` permet à un utilisateur mal intentionné de corrompre le contenu du fichier des mots de passe ou d'empêcher tout accès ultérieur à celui-ci. Ceci a pour effet de produire un déni de service sur la gestion des imprimantes.

CAN-2004-1270 Le programme `lppasswd` permet à un utilisateur malicieux capable de produire un message d'erreur astucieusement construit de modifier le contenu du fichier des mots de passe servant à la gestion des imprimantes.

5 Solution

Un correctif de sécurité est proposé par les différentes distributions.

6 Documentation

- le projet CUPS :
<http://www.cups.org> ;
- le correctif Red-HAT (RHSA-2005:013-20) :
<http://rhn.redhat.com/errata/RHSA-2005-013.html> ;
- le correctif Red-HAT (RHSA-2005:053-19) du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-053.html> ;
- le correctif Mandrake (MDKSA-2005:008) :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:008>

Gestion détaillée du document

19 janvier 2005 version initiale.

17 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:053.