



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 octobre 2004  
N° CERTA-2004-AVI-322-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du filtre d'impression foomatic-rip

---

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-2004-AVI-322>

---

### Gestion du document

Référence	CERTA-2004-AVI-322-001
Titre	Vulnérabilité du filtre d'impression foomatic-rip
Date de la première version	21 septembre 2004
Date de la dernière version	11 octobre 2004
Source(s)	Bulletin de sécurité SuSE SuSE-SA:2004:031 Bulletin de sécurité Mandrake MDKSA-2004:094
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 commandes arbitraires à distance.

## 2 Systèmes affectés

Versions de Foomatic antérieures à la version 3.0.2.

## 3 Description

Une vulnérabilité présente dans Foomatic-rip, un filtre d'impression, peut être exploitée par un utilisateur mal intentionné lors de la soumission d'une requête d'impression afin d'exécuter des commandes arbitraires sur le serveur d'impression.

## 4 Contournement provisoire

Filter les accès au serveur d'impression afin de limiter l'exploitation de cette vulnérabilité.

## 5 Solution

La version 3.0.2 de `Foomatic` corrige cette vulnérabilité.

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

## 6 Documentation

- Annonce de la version 3.0.2 de `Foomatic` :  
<http://www.linuxprinting.org/pipermail/foomatic-devel/2004q3/001996.html>
- Bulletin de sécurité Mandrake MDKSA-2004:094 du 15 septembre 2004 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:094>
- Bulletin de sécurité SuSE SuSE-SA:2004:031 du 15 septembre 2004 :  
[http://www.suse.com/de/security/2004\\_31\\_cups.html](http://www.suse.com/de/security/2004_31_cups.html)
- Bulletin de sécurité Gentoo GLSA 200409-24 du 20 septembre 2004 :  
<http://security.gentoo.org/glsa/glsa-200409-24.xml>
- Bulletin de sécurité Sun #57646 du 07 octobre 2004 :  
<http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-57646-1>
- Référence CVE CAN-2004-0801 :  
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CAN-2004-0801>

## Gestion détaillée du document

**21 septembre 2004** version initiale.

**11 octobre 2004** ajout référence au bulletin de Sun.