



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 décembre 2006  
N° CERTA-2006-AVI-556

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de GNOME Display Manager (GDM)

---

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-2006-AVI-556>

---

### Gestion du document

Référence	CERTA-2006-AVI-556
Titre	Vulnérabilité de GNOME Display Manager (GDM)
Date de la première version	15 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense 453 du 14 décembre 2006
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

Les versions de GNOME Display Manager (GDM) antérieures à 2.14.11, 2.16.4 ou 2.17.4.

## 3 Description

Une vulnérabilité a été identifiée dans GNOME Display Manager (GDM), qui ne manipulerait pas correctement une chaîne de caractères utilisée par `gdmchooser`, une fonction servant à sélectionner les hôtes activés par XDMCP sur le réseau local (XDMCP, pour *X Display Manager Control Protocol*).

Une personne malveillante connectée au système ayant une version de `gdmchooser` vulnérable pourrait exécuter du code arbitraire localement, avec les mêmes droits que ceux de l'utilisateur `gdm`.

## 4 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

## **5 Documentation**

- Article 453 de iDefense du 14 décembre 2006 :  
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=453>
- Bulletin de sécurité Mandriva MDKSA-2006:231 du 14 décembre 2006 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:231>
- Référence CVE CVE-2006-6105 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6105>

### **Gestion détaillée du document**

**15 décembre 2006** version initiale.