Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 octobre 2003
N° CERTA-2003-AVI-174

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Déni de service dans GDM



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2003-AVI-174 |
| Titre | Déni de service dans GDM |
| Date de la première version | 27 octobre 2003 |
| Date de la dernière version | – |
| Source(s) | CVE : CAN-2003-0793<br>CVE : CAN-2003-0794<br>Mandrake : MDKSA-2003:100 |
| 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 ;
- Impossibilité de se connecter au travers de l'interface `gdm`.

## 2 Systèmes affectés

- Pour GNOME 2.2 : versions antérieures à 2.4.1.7 ;
- pour GNOME 2.4 : versions antérieures à 2.4.4.4.

## 3 Résumé

Deux vulnérabilités dans certaines versions du logiciel de connexion `gdm` peuvent provoquer des dénis de service pouvant empêcher un utilisateur légitime de se connecter.

# 4 Description

*Gnome Display Manager* (`gdm`) est un logiciel de gestion des sessions *XWindows* qui présente une fenêtre de connexion.

Deux vulnérabilités dans `gdm` permettent de provoquer un déni de service sur la machine sur laquelle tourne ce logiciel :

1° un utilisateur peut exploiter une caractéristique de `gdm` dans le but d'épuiser la mémoire disponible, ce qui aura pour effet de tuer le processus `gdm`.

2° une limitation dans la gestion des commandes traitées par `gdm` peut être exploitée afin de saturer `gdm` de commandes inutiles, rendant impossible le traitement de commandes ultérieures valides (comme par exemple une demande de connexion).

# 5 Solution

Les utilisateurs de `gdm` sont invités à migrer vers une version qui corrige ces vulnérabilités, c'est-à-dire :

- à partir des sources appliquer une version supérieure ou égale à 2.4.1.7 ou 2.4.4.4 ;
- à partir d'un correctif fourni par votre vendeur, prendre le correctif qui corrige les vulnérabilités CAN-2003-0793 et CAN-2003-0794.

`gdm` tourne sous la forme d'un *daemon*. Installer le correctif peut ne pas suffire si la version vulnérable tourne encore en mémoire. Assurez-vous de bien redémarrer le *daemon* `gdm`.

# 6 Documentation

- Le site de référence du projet `gdm` :
  http://www.jirka.org/gdm
- Référence aux deux vulnérabilités dans la base CVE :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0793
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0794
- Avis de sécurité Mandrake MDKSA:100
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:100

# Gestion détaillée du document

**27 octobre 2003** version initiale.