Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mars 2002
N° CERTA-2002-AVI-059-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur les gestionnaires d'affichage X11 utilisant le protocole XDMCP

Gestion du document

Référence	CERTA-2002-AVI-059-001
Titre	Vulnérabilité sur les gestionnaires d'affichage X11 utilisant le protocole XDMCP
Date de la première version	21 mars 2002
Date de la dernière version	22 mars 2002–
Source(s)	Note VU#634847 du CERT/CC –
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

Divulgation d'informations.

2 Systèmes affectés

- SUN Solaris 2.6 et 7 ;
- Mandrake 8.0 et versions antérieures.

3 Résumé

Une vulnérabilité a été trouvée dans la configuration par défaut des gestionnaire d'affichage X11 implémentant XDCMP.

4 Description

Lors de l'installation certains gestionnaires d'affichage X11 utilisant le protocole XDMCP (X Display Manager Control Protocol) sont configurés par défaut afin de permettre des connexions distantes depuis n'importe quel autre

client. Lors de cette demande de connexion, la liste des utilisateurs autorisés à ouvrir une session est divulguée.

5 Contournement provisoire

- Filtrer le port du protocole XDMCP (UDP/177) en n'acceptant que les connexions par des utilisateurs autorisés.
- Désactiver les connexions distantes si elles ne sont pas utilisées dans le fichier de configuration "Xaccess"

```
#* #any host can get a login window
#* CHOOSER BROADCAST #any indirect host can get a chooser
```

6 Documentation

- Note du CERT/CC VU#634847
  http://kb.cert.org/vuls/id/634847
- Bulletin de sécurité Mandrake MDKSA-2002:025
  http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-025.php

Gestion détaillée du document

21 mars 2002 version initiale.
22 mars 2002 première révision : ajout de l'avis Mandrake MDKSA-2002:025.