

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de XFree86

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-211>

Gestion du document

| | |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Référence | CERTA-2004-AVI-211-002 |
| Titre | Vulnérabilité de XFree86 |
| Date de la première version | 30 juin 2004 |
| Date de la dernière version | 28 juillet 2004 |
| Source(s) | Bulletin de sécurité FreeBSD pour XFree86 du 28 juin 2004 Bulletin de sécurité OpenBSD pour XFree86 du 26 mai 2004 |
| 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.

2 Systèmes affectés

Toutes les versions de XFree86.

3 Résumé

Une vulnérabilité présente dans le gestionnaire d'environnement graphique XDM de XFree86 permet à un utilisateur distant mal intentionné de se connecter au serveur même si celui-ci a été désactivé.

4 Description

XDM est un gestionnaire d'environnement graphique présent dans XFree86. Il permet de créer des sessions sur des plates-formes distantes via le protocole XDMCP (X Display Manager Control Protocol). Une vulnérabilité de XDM autorise les connexions distantes au serveur X même si celles-ci ont été désactivées dans le fichier de

configuration `xm-config`. Cette vulnérabilité peut être exploitée par un individu mal intentionné afin d'accéder au serveur à distance.

5 Solution

Mettre à jour XFree86 (cf. section Documentation).

6 Documentation

- Site Internet de XFree86 :
<http://www.xfree86.org>
- Bulletin de sécurité Gentoo GLSA 200407-05 du 05 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-05.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:073 du 27 juillet 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:073>
- Bulletin de sécurité FreeBSD pour XFree86 du 28 juin 2004 :
<http://www.vuxml.org/freebsd>
- Bulletin de sécurité OpenBSD pour XFree86 du 26 mai 2004 :
<http://www.openbsd.org/errata.html#xwm>
- Description de la vulnérabilité XFree86 dans Bugzilla :
http://bugs.xfree86.org/show_bug.cgi?id=1376
- Référence CVE CAN-2004-0419 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CAN-2004-0419>

Gestion détaillée du document

30 juin 2004 version initiale.

06 juillet 2004 ajout de la référence au bulletin de sécurité Gentoo, de la référence CVE et du site Internet de XFree86.

28 juillet 2004 ajout de la référence au bulletin de sécurité Mandrake.