



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 26 septembre 2005  
N° CERTA-2005-AVI-345-003

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Xfree86/X11/Xorg

---

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-2005-AVI-345>

---

### Gestion du document

|                             |                                     |
|-----------------------------|-------------------------------------|
| Référence                   | CERTA-2005-AVI-345-003              |
| Titre                       | Vulnérabilité dans Xfree86/X11/Xorg |
| Date de la première version | 15 septembre 2005                   |
| Date de la dernière version | 26 septembre 2005                   |
| Source(s)                   | Bulletin de sécurité Gentoo         |
| 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

- Augmentation de privilèges ;
- exécution de code arbitraire.

## 2 Systèmes affectés

- Xfree86 version 4.1.x ;
- Xfree86 version 4.2.x ;
- Xfree86 version 4.3.x ;
- Xfree86 version 4.4.x ;
- Xfree86 version 4.5.x ;
- X11 6.X.

## 3 Description

Une vulnérabilité a été découverte dans Xfree86/X11/Xorg. Cette vulnérabilité peut être exploitée en local. L'exploitation permet l'exécution de code arbitraire qui peut conduire à l'obtention de nouveaux privilèges.

## 4 Solution

Mettre à jour via les mécanismes mis à disposition par l'éditeur du système d'exploitation.

## 5 Documentation

- Bulletin de sécurité Gentoo GLSA-200509-07 du 12 septembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200509-07.xml>
- Bulletin de sécurité RedHat RHSA-2005-329 du 12 septembre 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-329.html>
- Bulletin de sécurité RedHat RHSA-2005-396 du 13 septembre 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-396.html>
- Bulletins de sécurité FreeBSD pour XFree86-Server et xorg-server du 15 septembre 2005 :  
<http://www.vuxml.org/freebsd/pkg-XFree86-Server.html>  
<http://www.vuxml.org/freebsd/pkg-xorg-server.html>
- Bulletin de sécurité Sun #101926 du 15 septembre 2005 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101926-1>
- Bulletin de sécurité Mandriva MDKSA-2005:164 du 13 septembre 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:164>
- Bulletin de sécurité Debian DSA-816 du 19 septembre 2005 :  
<http://www.debian.org/security/2005/dsa-816>
- Bulletin de sécurité SUSE SUSE-SA-2005:056 du 26 septembre 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_56\\_xserver.html](http://www.novell.com/linux/security/advisories/2005_56_xserver.html)
- Référence CVE CAN-2005-2495 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2495>

## Gestion détaillée du document

**15 septembre 2005** version initiale.

**19 septembre 2005** ajout de la référence CVE CAN-2005-2495 et des références aux bulletins de sécurité FreeBSD, Sun, RedHat RHSA-2005-396 et Mandriva.

**22 septembre 2005** ajout de la référence au bulletin de sécurité Debian DSA-816.

**26 septembre 2005** ajout de la référence au bulletin de sécurité SUSE SUSE-SA-2005:056.