

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans libXfont

---

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-2011-AVI-673>

---

### Gestion du document

Référence	CERTA-2011-AVI-673
Titre	Vulnérabilité dans libXfont
Date de la première version	06 décembre 2011
Date de la dernière version	–
Source	Bulletin de sécurité Novell CVE-2011-2895 du 05 décembre 2011
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

Élévation de privilèges.

## 2 Systèmes affectés

libXfont, version 1.4.3 et versions antérieures.

## 3 Résumé

Une vulnérabilité dans libXfont permet à un utilisateur malveillant d'élever ses privilèges.

## 4 Description

La bibliothèque libXfont utilise un programme de décompression LZW vulnérable à un débordement de mémoire. Ce défaut peut être exploité par un utilisateur malveillant pour obtenir les droits de l'application ayant utilisé cette bibliothèque, par exemple un serveur X.

## 5 Solution

La version 1.4.4 de la bibliothèque libXfont corrige ce problème.

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

## 6 Documentation

- Bulletin de sécurité X.org du 10 août 2011 :  
<http://lists.freedesktop.org/archives/xorg-announce/2011-August/001721.html>
- Bulletin de sécurité Debian DSA 2293 du 12 août 2011 :  
<http://www.debian.org/security/2011/dsa-2293>
- Bulletin de sécurité Mandriva MDKSA-2011:153 du 17 octobre 2011 :  
<http://www.mandriva.com/archives/security/advisories>
- Correctif de sécurité NetBSD SA2011-007 du 20 septembre 2011 :  
<http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2011-007.txt.asc>
- Bulletin de sécurité RedHat RHSA-2011:1154 du 11 août 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-1154.html>
- Bulletin de sécurité RedHat RHSA-2011:1155 du 11 août 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-1155.html>
- Bulletin de sécurité RedHat RHSA-2011:1161 du 15 août 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-1161.html>
- Bulletin de sécurité Novell CVE-2011-2895 du 05 décembre 2011 :  
<http://support.novell.com/security/cve/CVE-2011-2895.html>
- Bulletin de sécurité Ubuntu USN-1191-1 du 15 août 2011 :  
<http://www.ubuntu.com/usn/usn-1191-1/>
- Référence CVE CVE-2011-2895 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2895>

## Gestion détaillée du document

06 décembre 2011 version initiale.