

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de XFree86 et Xsun

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-034>

Gestion du document

Référence	CERTA-2004-AVI-034-007
Titre	Multiples vulnérabilités de XFree86 et XSun
Date de la première version	12 février 2004
Date de la dernière version	03 juin 2005
Source(s)	Bulletin de sécurité 02.10.04 d'iDEFENSE Bulletin de sécurité 200402-02 de 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

Elévation de privilèges.

2 Systèmes affectés

XFree86 versions 4.3.0 et antérieures.
Xsun et Xprt sous Solaris sont également vulnérables.

3 Description

XFree86 est une mise en oeuvre du système X Window très utilisée sur les plates-formes Linux.
Xsun est le serveur X11 sous Solaris. Xprt est un serveur d'impression sous Solaris.

Deux vulnérabilités de type débordement de mémoire sont présentes dans le code réalisant l'analyse du fichier `font.alias`.

Par le biais d'un fichier `font.alias` habilement constitué, un utilisateur mal intentionné peut exploiter une de ces vulnérabilités afin d'obtenir les privilèges du super-utilisateur `root` sur la plate-forme vulnérable.

4 Solution

Appliquer le correctif disponible sur [ftp.xfree86.org](ftp://ftp.xfree86.org) :
<ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff>
ou réaliser la mise à jour du paquetage XFree86 :

- Bulletin de sécurité 200402-02 de Gentoo :
<http://www.securityfocus.com/advisories/6313>
- Bulletin de sécurité RHSA-2004:059 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-059.html>
- Bulletin de sécurité MDKSA-2004:012 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:012>
- Bulletin de sécurité IY53508 d'IBM pour AIX 4.3.3 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY53508>
- Bulletin de sécurité IY53673 d'IBM pour AIX 5.1.0 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY53673>
- Bulletin de sécurité IY53519 d'IBM pour AIX 5.2.0 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY53519>
- Bulletin de sécurité d'OpenBSD :
<http://www.openbsd.org/errata.html#font>
- Bulletin de sécurité Suse :
http://www.suse.com/de/security/2004_06_xf86.html
- Bulletin de sécurité HPSBUX01018 de Hewlett-Packard :
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0551.1>
- Bulletin de sécurité FreeBSD du 12 février 2004 :
<http://www.vuxml.org/freebsd>

Bulletin de sécurité Sun #57768 du 18 mai 2005 :
<http://www.sunsolve.com/search/document.do?assetkey=1-26-57768-1>

5 Documentation

- Bulletin de sécurité 02.10.04 d'iDEFENSE :
<http://www.iddefense.com/application/poi/display?id=72>
- Bulletin de sécurité 02.12.04 d'iDEFENSE :
<http://www.iddefense.com/application/poi/display?id=73>
- Référence CVE CAN-2004-0083 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0083>
- Référence CVE CAN-2004-0084 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0084>

Gestion détaillée du document

12 février 2004 version initiale.

13 février 2004 Prise en compte du second bulletin de sécurité d'iDEFENSE. Ajout référence au bulletin de sécurité de Red Hat.

16 février 2004 Ajout référence au bulletin de sécurité de Mandrake.

19 février 2004 Ajout référence aux bulletins de sécurité d'IBM et OpenBSD.

24 février 2004 Ajout référence au bulletin Suse.

29 avril 2004 Ajout référence au bulletin de Hewlett-Packard.

13 mai 2004 Ajout du bulletin de sécurité FreeBSD.

03 juin 2005 Nouveau titre. Ajout référence au bulletin de sécurité de Sun.