

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans X.Org

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-2007-AVI-424>

Gestion du document

Référence	CERTA-2007-AVI-424-002
Titre	Multiples vulnérabilités dans X.Org
Date de la première version	04 octobre 2007
Date de la dernière version	16 janvier 2008
Source(s)	Bulletin de sécurité de X.Org du 02 octobre 2007
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

– X.org XFS versions 1.0.4 et antérieures.

3 Résumé

De multiples vulnérabilités ont été découvertes dans X.Org XFS permettant l'exécution de code arbitraire à distance.

4 Description

Deux vulnérabilités, existant dans X.Org XFS, permettent l'exécution de code arbitraire à distance par un individu malveillant :

- la première des vulnérabilités permet un débordement d'entier via la fonction `build_range()` ;
- pour la seconde, un nombre arbitraire de `bits` permet un dépassement de mémoire dans la fonction `swap_char2b()`.

5 Solution

Se référer au bulletin de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité de X.Org du 02 octobre 2007 :
<http://lists.freedesktop.org/archives/xorg-announce/2007-October/000416.html>
- Bulletin de sécurité Debian du 09 octobre 2007:
<http://www.debian.org/security/2007/dsa-1385>
- Bulletin de sécurité Mandriva du 06 novembre 2007:
<http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:210>
- Bulletin de sécurité Gentoo du 12 octobre 2007:
<http://www.gentoo.org/security/en/glsa/glsa-200710-11.xml>
- Bulletin de sécurité SUSE du 12 octobre 2007:
http://www.novell.com/linux/security/advisories/2007_54_xorg.html
- Bulletin de sécurité Sun du 06 novembre 2007:
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103114-1>
- Bulletin de sécurité HP-UX du 14 janvier 2008:
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01323725>
- Bulletin de sécurité de iDefense du 02 octobre 2007 :
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=602>
- Référence CVE CVE-2007-4568 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4568>
- Référence CVE CVE-2007-4990 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4990>

Gestion détaillée du document

04 octobre 2007 version initiale.

07 novembre 2007 ajout de la référence CVE et des références aux bulletins de sécurité Mandriva, Gentoo, SUSE et Sun.

16 janvier 2008 ajout de la référence au bulletin de sécurité HP-UX.