Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juin 2007
N° CERTA-2007-AVI-025-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de X.org

Gestion du document

Référence	CERTA-2007-AVI-025-003
Titre	Multiples vulnérabilités de X.org
Date de la première version	10 janvier 2007
Date de la dernière version	19 juin 2007
Source(s)	Bulletins de sécurité iDefense 463 à 465
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

- X Window System 11 (X11) 6.X ;
- X Window System 11 (X11) 7.X.
- Xfree86 4.1.x ;
- Xfree86 4.2.x ;
- Xfree86 4.3.x ;
- Xfree86 4.4.x ;
- Xfree86 4.5.x ;
- Xfree86 4.6.x ;

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans `X.org`. Ces vulnérabilités peuvent être exploitées afin d'obtenir une élévation de privilèges.

4 Description

Trois vulnérabilités ont été découvertes dans `X.org`. Ces vulnérabilités sont dues à une erreur dans le traitement des entrées des fonctions *ProcRenderAddGlyphs()*, *ProcDbeSwapBuffers()* et *ProcDbeGetVisualInfo()*. Ces vulnérabilités peuvent être exploitées par un utilisateur malintentionné afin d'obtenir les privilèges de l'utilisateur sous lequel est lancé le serveur X (en général, *root*).

Un système ne présente ces vulnérabilités que s'il est configuré avec les extensions `DBE` et `Render` (l'extension `Render` est installée par défaut).

5 Solution

Se référer au bulletin de sécurité des éditeurs pour l'obtention des correctifs, ou installer la version 7.2RC3 du serveur `X.org` (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2007-005 du 09 janvier 2007 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007-005
- Bulletin de sécurité RedHat RHSA-2007:0003 du 10 janvier 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0003.html
- Bulletin de sécurité Suse SUSE-SA:2007:008 du 12 janvier 2007 :
  http://support.novell.com/techcenter/pdsb/380666439b7217bd698fe6e5213851c.html
- Bulletin de sécurité iDefense du 09 janvier 2007 :
  http://www.idefense.com/application/poi/display?id=463
- Bulletin de sécurité iDefense du 09 janvier 2007 :
  http://www.idefense.com/application/poi/display?id=464
- Bulletin de sécurité iDefense du 09 janvier 2007 :
  http://www.idefense.com/application/poi/display?id=465
- Bulletin de sécurité de HP HPSPBUX02225 du 12 juin 2007 :
  http://h20000.www.2.hp.com/bizsupport/techSupport/Document.jsp?objectID=c01075678
- Référence CVE CVE-2006-6101 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6101
- Référence CVE CVE-2006-6102 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6102
- Référence CVE CVE-2006-6103 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6103
- Bulletin de sécurité Gentoo GLSA 200701-25 du 27 janvier 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200701-25.xml
- Bulletin de sécurité Debian DSA-1249 du 15 janvier 2007 :
  http://www.us.debian.org/security/2007/dsa-1249

Gestion détaillée du document

10 janvier 2007 version initiale.
15 janvier 2007 systèmes affectés et référence Suse.
30 janvier 2007 ajout des références aux bulletins de sécurité Gentoo et Debian.
19 juin 2007 ajout de la référence au bulletin HP.