



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 décembre 2006
N° CERTA-2006-AVI-397-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans X.org X11 et XFree86

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-2006-AVI-397>

Gestion du document

Référence	CERTA-2006-AVI-397-002
Titre	Plusieurs vulnérabilités dans X.org X11 et XFree86
Date de la première version	14 septembre 2006
Date de la dernière version	18 décembre 2006
Source(s)	Bulletin de sécurité RedHat RHSA-2006-0665 du 12 septembre 2006
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 ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- X.Org X11 6.8.2 ;
- X.Org X11 6.9.0 ;
- X.Org X11 7.0 ;
- X.Org X11 7.1 ;
- XFree86 4.6.0.

3 Description

Des vulnérabilités ont été identifiées dans les services graphiques X.Org X11 et XFree86. Ils ne manipuleraient pas correctement des caractères CID (pour *Character Identifier*) de Type 1. Les fonctions mises en cause sont :

- Type1/scanfont.c

- Type1/afm.c

Il est cependant possible de restreindre les formats de caractères dans le fichier de configuration de ces applications (par exemple dans : `/etc/X11/xorg.conf`) en activant le seul module `freetype`, et en désactivant le module posant problème `type1`.

Un utilisateur local au système pourrait exploiter ces vulnérabilités, sous certaines conditions, en obligeant le serveur X.Org X11 ou XFree86 à interpréter les caractères impliqués. Il pourrait alors provoquer un déni de service ou exécuter des commandes arbitraires sur le système vulnérable avec les droits du serveur (souvent associés à ceux de l'administrateur).

4 Solution

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

5 Documentation

- Bulletin de sécurité RedHat RHSA-2006:0665 du 12 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0665.html>
- Bulletin de sécurité RedHat RHSA-2006:0666 du 12 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0666.html>
- Bulletin de sécurité Ubuntu USN-344-1 du 12 septembre 2006 :
<http://www.ubuntu.com/usn/usn-344-1>
- Bulletin de sécurité Gentoo GLSA-200609-07 du 13 septembre 2006 :
<http://www.gentoo.org/security/en/glsa-200609-07.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:164 du 14 septembre 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:164>
- Bulletin de sécurité Avaya ASA-2006-191 du 23 octobre 2006 :
<http://support.avaya.com/elmodocs2/security/ASA-2006-191.html>
- Bulletin de sécurité Avaya ASA-2006-190 du 26 septembre 2006 :
<http://support.avaya.com/elmodocs2/security/ASA-2006-190.html>
- Avis de sécurité X.Org du 12 septembre 2006 :
<http://wiki.x.org/wiki/SecurityPage>
- Mises à jour de XFree86 :
<http://www.xfree86.org/releases/rel460.html>
- Référence CVE CVE-2006-3739 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3739>
- Référence CVE CVE-2006-3740 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3740>

Gestion détaillée du document

14 septembre 2006 version initiale.

25 octobre 2006 ajout de la référence au bulletin de sécurité Avaya.

18 décembre 2006 ajout des références aux bulletins de sécurité Avaya, Red Hat et Gentoo.