



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 mai 2007
N° CERTA-2007-AVI-177-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans X.Org 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-2007-AVI-177>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2007-AVI-177-002 |
| Titre | Multiples vulnérabilités dans X.Org et XFree86 |
| Date de la première version | 16 avril 2007 |
| Date de la dernière version | 07 mai 2007 |
| Source(s) | Bulletins de sécurité iDefense #501, #502 et #503 |
| 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

- Déni de service ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- X.Org versions 7.1 et antérieures ;
- XFree86 versions 4.6 et antérieures.

3 Résumé

De multiples vulnérabilités dans X.Org et XFree86 permettent à un utilisateur local de provoquer un déni de service, de porter atteinte à la confidentialité des données ou d'élèver ses privilèges.

4 Description

Plusieurs vulnérabilités sont présentes dans les serveurs de rendu graphique XFree86 et X.Org :

- la première, de type débordement d’entier, concerne la gestion des polices de caractères au format BDF (Bitmap Description Format) et permettrait une élévation de privilèges ;
- la seconde, également de type débordement d’entier, est relative à la gestion des polices au format font.dir et permettrait une élévation de privilèges ;
- la troisième concerne un manque de contrôle dans la fonction *ProcXCMiscGetXIDList()* de l’extension XC-MISC et permettrait une élévation de privilèges ;
- la dernière est relative à la fonction *XGetPixel()* dans le fichier *ImUtil.c* et permettrait d’accéder de façon illégitime à certains fichiers du système.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Sun 102886 du 25 avril 2007 :
<http://sunsolve.com/search/document.do?assetkey=1-26-102886-1>
- Bulletin de sécurité Mandriva MDKSA-2007:079 du 04 avril 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:079>
- Bulletin de sécurité RedHat RHSA-2007:0126 du 03 avril 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0126.html>
- Bulletin de sécurité Ubuntu USN-448-1 du 03 avril 2007 :
<http://www.ubuntulinux.org/usn/usn-448-1>
- Bulletin de sécurité Gentoo GLSA 200705-06 du 05 mai 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200705-06.xml>
- Bulletin de sécurité SuSE SUSE-SR:2007:008 du 27 avril 2007 :
http://www.novell.com/linux/security/advisories/2007_8_sr.html
- Bulletin de sécurité SuSE SUSE-SR:2007:027 du 20 avril 2007 :
http://www.novell.com/linux/security/advisories/2007_27_x.html
- Bulletin de sécurité OpenBSD 3.9 du 04 avril 2007 :
http://www.openbsd.org/errata39.html#021_xorg
- Bulletin de sécurité OpenBSD 4.0 du 04 avril 2007 :
http://www.openbsd.org/errata40.html#011_xorg
- Bulletin de sécurité iDefense du 03 avril 2007 :
<http://www.iddefense.com/application/poi/display?id=501>
- Bulletin de sécurité iDefense du 03 avril 2007 :
<http://www.iddefense.com/application/poi/display?id=502>
- Bulletin de sécurité iDefense du 03 avril 2007 :
<http://www.iddefense.com/application/poi/display?id=503>
- Référence CVE CVE-2007-1003 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1003>
- Référence CVE CVE-2007-1351 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1351>
- Référence CVE CVE-2007-1352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1352>
- Référence CVE CVE-2007-1667 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1667>

Gestion détaillée du document

16 avril 2007 version initiale.

26 avril 2007 ajout de la référence Sun.

07 mai 2007 ajout des références OpenBSD, SuSE, et Gentoo.