



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 5 novembre 2008
N° CERTA-2008-AVI-030-001

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-2008-AVI-030>

Gestion du document

Référence	CERTA-2008-AVI-030-001
Titre	Multiples vulnérabilités dans X.Org
Date de la première version	18 janvier 2008
Date de la dernière version	5 novembre 2008
Source(s)	Bulletin de sécurité X.Org 031918 du 17 janvier 2008
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 ;
- déni de service à distance ;
- élévation de privilèges.

2 Systèmes affectés

- X Windows System 11 (X11) 6.x ;
- X Windows System 11 (X11) 7.x.

3 Résumé

Plusieurs vulnérabilités touchant le système X Windows, dues à la mauvaise validation de paramètres, ont été corrigées.

4 Description

Elles permettent entre autres d'exécuter du code arbitraire avec les droits du processus du *serveur X*. Pour mener à bien son attaque, l'utilisateur malveillant doit avoir accès à un shell local ou à une connexion déjà établie avec le *serveur X*.

5 Solution

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

6 Documentation

- Bulletin de sécurité HP-UX c01543321 du 3 novembre 2008:
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01543321>
- Bulletin de sécurité Gentoo GLSA 200801-09 du 20 janvier 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200801-09.xml>
- Bulletin de sécurité Debian DSA-1466 du 17 janvier 2008 :
<http://www.debian.org/security/2008/dsa-1466>
- Bulletin de sécurité Mandriva MDKSA-2008:023 du 23 janvier 2008 :
<http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:023>
- Bulletin de sécurité Mandriva MDKSA-2008:025 du 23 janvier 2008 :
<http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:025>
- Bulletin de sécurité RedHat RHSA-2008:0030 du 17 janvier 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0030.html>
- Bulletin de sécurité RedHat RHSA-2008:0031 du 17 janvier 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0031.html>
- Bulletin de sécurité RedHat RHSA-2008:0064 du 17 janvier 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0064.html>
- Bulletin de sécurité Ubuntu USN-571-1 du 18 janvier 2008 :
<http://www.ubuntu.com/usn/usn-571-1>
- Bulletin de sécurité Ubuntu USN-571-2 du 19 janvier 2008 :
<http://www.ubuntu.com/usn/usn-571-2>
- Bulletin de sécurité SuSE SUSE-SA:2008:003 du 17 janvier 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-01/msg00004.html>
- Bulletin de sécurité Sun Solaris #103192 du 17 janvier 2008 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103192-1>
- Bulletin de sécurité Sun Solaris #103200 du 17 janvier 2008 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103200-1>
- Bulletin de sécurité Sun Solaris #103205 du 17 janvier 2008 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103205-1>
- Bulletin de sécurité Ubuntu USN-571-1 du 17 janvier 2008 :
<http://www.ubuntulinux.org/usn/usn-571-1>
- Bulletin de sécurité Suse SUSE-SA:2008:003 du 17 janvier 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-01/msg00004.html>
- Bulletin de sécurité Avaya ASA-2008-039 du 28 janvier 2008 :
<http://support.avaya.com/elmodocs2/security/ASA-2008-039.htm>
- Bulletin de sécurité iDefense 643 du 17 janvier 2008 :
<http://www.iddefense.com/ntelligence/vulnerabilities/display.php?id=643>
- Bulletin de sécurité iDefense 645 du 17 janvier 2008 :
<http://www.iddefense.com/ntelligence/vulnerabilities/display.php?id=645>
- Bulletin de sécurité iDefense 646 du 17 janvier 2008 :
<http://www.iddefense.com/ntelligence/vulnerabilities/display.php?id=646>

- Référence CVE CVE-2007-5760 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5760>
- Référence CVE CVE-2007-5958 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5958>
- Référence CVE CVE-2007-6427 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6427>
- Référence CVE CVE-2007-6428 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6428>
- Référence CVE CVE-2007-6429 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6429>
- Référence CVE CVE-2008-0006 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0006>

Gestion détaillée du document

18 janvier 2008 version initiale.

11 février 2008 ajout des références aux bulletins de sécurité Mandriva, Ubuntu, Debian, Gentoo, SuSE et Avaya.

5 novembre 2008 ajout de la référence au bulletin de sécurité HP-UX.