



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mars 2006
N° CERTA-2006-AVI-120-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur X.Org-X11

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-120>

Gestion du document

Référence	CERTA-2006-AVI-120-001
Titre	Vulnérabilité du serveur X.Org-X11
Date de la première version	21 mars 2006
Date de la dernière version	22 mars 2006
Source(s)	Bulletin de sécurité de l'éditeur
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 ;
- élévation de privilèges.

2 Systèmes affectés

Les versions X.Org server 1.0.0, X11R6.9 et X11R7.0.

3 Résumé

Une vulnérabilité dans la vérification des privilèges des serveurs graphiques X.Org 1.0.0, X11R6.9 et X11R7.0 permet à un utilisateur malveillant d'exécuter du code arbitraire et d'obtenir les privilèges de l'administrateur.

4 Description

Une erreur dans la vérification des privilèges de l'utilisateur effectuée par la fonction `getuid` des serveurs graphiques X.Org 1.0.0, X11R6.9 et X11R7.0 permet à un utilisateur malveillant ayant accès à la machine d'introduire des arguments arbitraires avec les options `-logfile` ou `-modulepath`. En d'autres termes, cette

vulnérabilité peut être utilisée pour écraser des fichiers existants ou exécuter du code arbitraire avec les privilèges de l'administrateur.

5 Solution

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

6 Documentation

- Site officiel du projet X.Org :
<http://xorg.freedesktop.org/releases/>
- Mise à jour de sécurité Fedora Core 5 du 21 mars 2006 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/5/>
- Bulletin de sécurité Mandriva MDKSA-2006:056 du 21 mars 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:056>
- Bulletin de sécurité Sun Solaris #102252 du 21 mars 2006 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102252-1>
- Bulletin de sécurité SUSE SUSE-SA:2006:016 du 21 mars 2006 :
http://www.novell.com/linux/security/advisories/2006_16_xorgx11server.html
- Bulletin de sécurité FreeBSD pour xorg-server du 21 mars 2006 :
<http://www.vuxml.org/freebsd/pkg-xorg-server.html>
- Référence CVE CVE-2006-0745 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2006-0745>

Gestion détaillée du document

21 mars 2006 version initiale.

22 mars 2006 ajout des références aux bulletins de sécurité SUSE et FreeBSD.