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 novembre 2006
N° CERTA-2006-AVI-480

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des drivers NVidia

Gestion du document

Référence	CERTA-2006-AVI-480
Titre	Vulnérabilité des drivers NVidia
Date de la première version	07 novembre 2006
Date de la dernière version	–
Source(s)	Notes de révision des pilotes NVidia 1.0-8776 pour Unix du 19 octobre 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 à distance.

2 Systèmes affectés

- Les pilotes NVidia pour GNU/Linux (architecture IA-32) versions 1.0-8774 et antérieures ;
- les pilotes NVidia pour GNU/Linux (architecture AMD64/EM64T) versions 1.0-8774 et antérieures ;
- les pilotes NVidia pour FreeBSD (architecture x86) versions 1.0-8774 et antérieures ;
- les pilotes NVidia pour Sun Solaris 10 (architectures x86 et x64) versions 1.0-8774 et antérieures.

3 Résumé

Une vulnérabilité dans les pilotes propriétaires pour les cartes graphiques NVidia permet à un utilisateur distant d'exécuter du code arbitraire à distance.

4 Description

NVidia fournit pour un certain nombre d'Unix dont GNU/Linux et FreeBSD des pilotes propriétaires, sous forme binaire uniquement, permettant d'utiliser les fonctions 3D des cartes graphiques basées sur les GPU (Graphic Processor Unit) NVidia. Une vulnérabilité de type débordement de mémoire présente dans ces pilotes permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance si le serveur X (Xorg ou XFree) utilisant les pilotes vulnérables accepte les connexions distantes. Si ce n'est pas le cas, l'exploitation de la vulnérabilité ne peut se faire que localement.

5 Solution

La version 1.0-8776 corrige le problème :
http://www.nvidia.com/object/unix.html

6 Documentation

- Notes de révision des pilotes NVidia 1.0-8776 pour Unix du 19 octobre 2006 :
  http://www.nvidia.com/object/linux_display_ia32_1.0-8776.html
  http://www.nvidia.com/object/linux_display_amd64_1.0-8776.html
  http://www.nvidia.com/object/freebsd_1.0-8776.html
  http://www.nvidia.com/object/solaris_display_1.0-8776.html
- Bulletin de sécurité Ubuntu USN-377-1 du 03 novembre 2006 :
  http://www.ubuntulinux.org/usn/usn-377-1
- Bulletin de sécurité Sun Solaris #102693 du 02 novembre 2006 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-102693-1
- Note de vulnérabilité de l'US-CERT VU#147252 du 17 octobre 2006 :
  http://www.kb.cert.org/vuls/id/147252
- Référence CVE CVE-2006-5379 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5379

Gestion détaillée du document

07 novembre 2006 version initiale.