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 janvier 2013
N° CERTA-2012-ALE-009-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans les pilotes NVidia

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-2012-ALE-009

Gestion du document

Référence	CERTA-2012-ALE-009-001
Titre	Vulnérabilité dans les pilotes NVidia
Date de la première version	26 décembre 2012
Date de la dernière version	07 janvier 2013
Source(s)	-
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 ;
- élévation de privilèges.

2 Systèmes affectés

Pilote NVidia version 310.70 pour *Microsoft Windows 7 64bit*. D'autres systèmes et versions sont probablement vulnérables.

3 Résumé

Une vulnérabilité a été découverte dans le service *NVidia Driver Helper Service* installé par les pilotes de carte graphique *NVidia*. Elle concerne un débordement de mémoire tampon pouvant mener un utilisateur malintentionné à exécuter du code arbitraire à distance.
Cette vulnérabilité peut être exploitée à distance au moyen du canal nommé *\pipe\nvsr*. Un exploit fonctionnel est largement diffusé sur Internet. Pour pouvoir être exploitée, cette vulnérabilité nécessite de posséder un compte disposant d'un accès légitime à la machine ; ce qui est généralement le cas des comptes utilisateurs d'un domaine. Cette vulnérabilité peut être également utilisée pour réaliser une élévation de privilèges en local.

4 Solution

NVidia a fourni une mise à jour vers la version 310.90 qui corrige la vulnérabilité.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité NVidia du 05 janvier 2013 :
  http://us.download.nvidia.com/Windows/310.90/310.90-win8-win7-winvista-desktop-release-notes-whql.pdf
- Téléchargement des pilotes GeForce 310.90 :
  http://www.geforce.com/drivers/results/55121

Gestion détaillée du document

26 décembre 2012 version initiale ;
07 janvier 2013 ajout du correctif éditeur, suppression du contournement provisoire.