



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2010
N° CERTA-2010-AVI-311

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du pilote d'affichage canonique dans Microsoft Windows

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-2010-AVI-311>

Gestion du document

Référence	CERTA-2010-AVI-311
Titre	Vulnérabilité du pilote d'affichage canonique dans Microsoft Windows
Date de la première version	15 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS10-043 du 13 juillet 2010
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.

2 Systèmes affectés

- Microsoft Windows 7 pour systèmes x64 ;
- Microsoft Windows Embedded Standard 7 pour systèmes x64 ;
- Microsoft Windows Server 2008 R2 pour systèmes x64.

3 Résumé

Une vulnérabilité du pilote d'affichage canonique dans Microsoft Windows permet à un utilisateur distant de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une vulnérabilité est présente dans le pilote d'affichage canonique dans Microsoft Windows : *cdd.dll*. Ce pilote sert, entre autres, à afficher les effets en 3D du bureau comme *Aero*. Cette faille permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire. Il est nécessaire que les effets 3D du bureau soient activés pour que l'exploitation soit fonctionnelle.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS10-043 du 13 juillet 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-043.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-043.msp>

Gestion détaillée du document

15 juillet 2010 version initiale.