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 juin 2011
N° CERTA-2011-AVI-354

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le composant AFD de Microsoft

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-2011-AVI-354

Gestion du document

Référence	CERTA-2011-AVI-354
Titre	Vulnérabilité dans le composant AFD de Microsoft
Date de la première version	15 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-046 du 14 juin 2011
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

Élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows XP SP ;
- Microsoft Windows XP Pro x64 SP2 ;
- Microsoft Windows Server 2003 SP2 (32bits, x64 et Itanium) ;
- Microsoft Windows Vista SP1 et SP2 (32bits et x64) ;
- Microsoft Windows Server 2008 (32bits, x64 et Itanium) ;
- Microsoft Windows Server 2008 SP2 (32bits, x64 et Itanium) ;
- Microsoft Windows Server 2008 R2 (x64 et Itanium) ;
- Microsoft Windows Server 2008 R2 SP1 (x64 et Itanium) ;
- Microsoft Windows 7 (32bits et x64) ;
- Microsoft Windows 7 SP1 (32bits et x64).

3 Résumé

Une vulnérabilité dans *Microsoft Windows Ancillary Function Driver* (AFD) a été corrigée et permet à un utilisateur malintentionné d'élever ses privilèges.

4 Description

Une vulnérabilité dans *Microsoft Windows Ancillary Function Driver* (AFD) due à une entrée non validée dans le noyau Windows a été corrigée. Elle permet à un utilisateur malintentionné disposant d'un compte sur la machine vulnérable d'élever ses privilèges au moyen d'un exécutable spécialement conçu.

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 MS11-046 du 14 juin 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-046.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-046.mspx
- Référence CVE CVE-2011-1249 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1249

Gestion détaillée du document

15 juin 2011 version initiale.