Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juillet 2012
N° CERTA-2012-AVI-380

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'interpréteur de commande 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-2012-AVI-380

Gestion du document

Référence	CERTA-2012-AVI-380
Titre	Vulnérabilité dans l'interpréteur de commande Windows
Date de la première version	11 juillet 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-048 du 10 Juillet 2012
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

- Windows XP Service Pack 3 ;
- Windows XP Professionnel Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 pour systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista Edition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 bits ;
- Windows 7 pour systèmes 32 bits Service Pack 1 ;
- Windows 7 pour systèmes x64 ;

- Windows 7 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes x64 ;
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium ;
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

3 Résumé

Une vulnérabilité a été corrigée dans l'interpréteur de commande *Windows*. Elle concerne la façon dont *Windows* gère les noms de fichiers et de répertoires et permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS12-048 du 10 juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-048
  http://technet.microsoft.com/en-us/security/bulletin/MS12-048
- Référence CVE CVE-2012-0175 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0175

Gestion détaillée du document

11 juillet 2012 version initiale.