



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 août 2010
N° CERTA-2010-AVI-374

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la pile TCP/IP de 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-374>

Gestion du document

Référence	CERTA-2010-AVI-374
Titre	Vulnérabilités dans la pile TCP/IP de Microsoft Windows
Date de la première version	11 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-058 du 10 août 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 ;
- élévation de privilèges ;
- déni de service à distance.

2 Systèmes affectés

- Windows Vista Service Pack 1 et Service Pack 2 ;
- Windows Vista x64 Service Pack 1 et Service Pack 2 ;
- Windows Server 2008 sans Service Pack et avec Service Pack 2 ;
- Windows Server 2008 x64 sans Service Pack et avec Service Pack 2 ;
- Windows Server 2008 Itanium sans Service Pack et avec Service Pack 2 ;
- Windows Server 2008 R2 x64 ;
- Windows Server 2008 R2 Itanium ;
- Windows 7 ;
- Windows 7 x64.

3 Résumé

Deux vulnérabilités ont été découvertes dans la pile TCP/IP de Microsoft Windows. Elles permettent de provoquer un déni de service à distance, d'exécuter du code arbitraire à distance, et d'élever ses privilèges.

4 Description

Deux vulnérabilités ont été découvertes dans la pile TCP/IP de Microsoft Windows :

- une erreur dans le traitement des en-têtes de paquets IPv6 permet de provoquer un déni de service à distance ;
- une erreur dans la gestion de réseau de Windows permet d'exécuter du code arbitraire à distance et d'élever ses privilèges.

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 MS10-058 du 10 août 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-058.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-058.msp>
- Référence CVE CVE-2010-1892 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1892>
- Référence CVE CVE-2010-1893 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1893>

Gestion détaillée du document

11 août 2010 version initiale.