



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 novembre 2011
N° CERTA-2011-AVI-621

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la pile TCP/IP de 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-2011-AVI-621>

Gestion du document

Référence	CERTA-2011-AVI-621
Titre	Vulnérabilité dans la pile TCP/IP de Windows
Date de la première version	09 novembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS-11-083 du 08 novembre 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Windows Vista Service Pack 2 ;
- Windows Server 2008 ;
- Windows Server 2008 R2 ;
- Windows 7.

3 Résumé

Une vulnérabilité dans la pile TCP/IP de Windows permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

La vulnérabilité est due à un dépassement d'entier (*integer overflow*) d'un compteur dans la pile TCP/IP de *Windows*. Cette vulnérabilité pourrait être exploitée par une personne malintentionnée en envoyant un grand nombre de paquets UDP spécialement conçus à destination d'un port qui n'est pas en écoute. Le traitement de ces paquets peut conduire à un dépassement d'entier d'un compteur de référence, et finalement mener à une exécution de code arbitraire à distance.

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 MS11-083 du 08 novembre 2011 :
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-083>
<http://technet.microsoft.com/en-us/security/bulletin/MS11-083>
- Référence CVE CVE-2011-2013 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2013>

Gestion détaillée du document

09 novembre 2011 version initiale.