



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2011
N° CERTA-2011-AVI-387

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la pile Bluetooth des systèmes 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-387>

Gestion du document

Référence	CERTA-2011-AVI-387
Titre	Vulnérabilité dans la pile Bluetooth des systèmes Windows
Date de la première version	13 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-053 du 12 juillet 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 1 et Windows Vista Service pack 2 pour systèmes 32 bits et x64 ;
- Windows 7 et Windows 7 Service pack 1 pour systèmes 32 bits et x64.

3 Résumé

Une vulnérabilité a été corrigée dans la pile Bluetooth des systèmes d'exploitation Windows Vista et Windows 7, qui permet d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été corrigée dans la pile Bluetooth des systèmes d'exploitation Windows Vista et Windows 7. Un attaquant envoyant une série de paquets Bluetooth spécialement conçus peut provoquer une exécution de code arbitraire avec des privilèges élevés. Cette vulnérabilité ne concerne que les systèmes équipés d'un composant réseau Bluetooth.

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 MS11-053 du 12 juillet 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-053.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-053.msp>
- Référence CVE CVE-2011-1265 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1265>

Gestion détaillée du document

13 juillet 2011 version initiale.