

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la pile Bluetooth 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-2008-AVI-303>

Gestion du document

Référence	CERTA-2008-AVI-303
Titre	Vulnérabilité de la pile Bluetooth Windows
Date de la première version	11 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-030 du 10 juin 2008
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 ;
- déni de service à distance.

2 Systèmes affectés

- Windows XP Service Pack 2 ;
- Windows XP Service Pack 3 ;
- Windows XP x64 Edition ;
- Windows XP x64 Edition Service Pack 2 ;
- Windows Vista ;
- Windows Vista Service Pack 1 ;
- Windows Vista x64 Edition ;
- Windows Vista x64 Edition Service Pack 1.

3 Résumé

Une vulnérabilité a été identifiée dans la mise en œuvre de la pile Bluetooth par Windows. Elle peut être exploitée par une personne malveillante à distance, via Bluetooth, pour exécuter du code arbitraire sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans la mise en œuvre de la pile Bluetooth par Windows. Sous certaines conditions, le système d'exploitation ne générerait pas correctement la réception de multiples trames SDP (*Service Discovery Protocol*). Ce protocole permet entre autres de déterminer la liste et les caractéristiques des services Bluetooth offerts par l'appareil distant.

La vulnérabilité peut être exploitée par une personne malveillante à distance pour exécuter du code arbitraire sur le système vulnérable. Le système doit *a fortiori* disposer d'une interface Bluetooth active.

5 Solution

Se référer au bulletin de sécurité MS08-030 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-030 du 10 juin 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-030.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-030.msp>
- Bloc-notes Microsoft, commentaires sur la mise à jour MS08-030 :
<http://blogs.microsoft.com/swi/archive/2008/06/10/ms08-030-all-bark-and-no-bite-the-case-of-the-bluetooth-update.aspx>
- Documentation officielle SDP sur le site SIG Bluetooth :
<http://www.bluetooth.org>
- Présentation du protocole SDP (Service Discovery Protocol) :
<http://www.palowireless.com/infetooth/tutorial/sdp.asp>
- Référence CVE CVE-2008-1453 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1453>

Gestion détaillée du document

11 juin 2008 version initiale.