



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 novembre 2009
N° CERTA-2009-AVI-490

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft WSDAPI

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-2009-AVI-490>

Gestion du document

Référence	CERTA-2009-AVI-490
Titre	Vulnérabilité de Microsoft WSDAPI
Date de la première version	10 novembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS09-063 du 10 novembre 2009
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

- Microsoft Windows Vista, Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Microsoft Windows Vista édition x64, Windows Vista édition x64 Service Pack 1 et Windows Vista édition x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2.

3 Résumé

Une vulnérabilité dans Microsoft Windows WSDAPI permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité est présente dans l'interface de programmation d'applications WSDAPI (Web Services on Devices API) disponible sur les systèmes Windows Vista et Windows 2008. Cette faille permet à un utilisateur malintentionné distant, mais sur le même sous-réseau, de provoquer un déni de service ou d'exécuter du code arbitraire sur le système vulnérable par le biais d'un paquet construit de façon particulière.

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 MS09-063 du 10 novembre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-063.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-063.msp>
- Référence CVE CVE-2009-2512 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2512>

Gestion détaillée du document

10 novembre 2009 version initiale.