



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 avril 2007
N° CERTA-2007-AVI-167

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Agent dans 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-2007-AVI-167>

Gestion du document

Référence	CERTA-2007-AVI-167
Titre	Vulnérabilité de Microsoft Agent dans Windows
Date de la première version	11 avril 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-020 du 10 avril 2007
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

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 compris).
- Microsoft Windows Server 2003 (Service Pack 1 et Service Pack 2 inclus) ;
- Microsoft Windows Server 2003 pour les systèmes Itanium (Service Pack 1 et Service Pack 2 inclus) ;
- Microsoft Windows Server 2003 x64 Edition (Service Pack 2 inclus) ;

3 Résumé

Une vulnérabilité a été identifiée dans le service Microsoft Agent de Windows. Une personne malveillante pourrait l'exploiter à distance pour prendre le contrôle total du système.

4 Description

Une vulnérabilité a été identifiée dans le service Microsoft Agent de Windows (`agentsvr.exe`). Celui-ci permet aux applications et certaines pages Web d'interagir avec l'utilisateur par le biais de personnages animés, qui peuvent bouger, émettre ou comprendre des sons, afficher des messages, etc.

Les adresses réticulaires (URL) ne seraient pas correctement contrôlées. Une personne malveillante pourrait donc, par le biais d'un site Web ou d'une application particulière, prendre le contrôle total d'un système vulnérable, dès lors que l'utilisateur visite la page ou utilise l'application.

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 MS07-020 du 10 avril 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-020.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-020.msp>
- Référence CVE CVE-2007-1205 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1205>
- Annonce du laboratoire de recherche Secunia :
http://secunia.com/secunia_research/2006-74

Gestion détaillée du document

11 avril 2007 version initiale.