

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Agent

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-2006-AVI-497>

Gestion du document

Référence	CERTA-2006-AVI-497
Titre	Vulnérabilité de Microsoft Agent
Date de la première version	15 novembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-068 du 14 novembre 2006
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 ;
- Microsoft Windows Server 2003 et Windows Server 2003 Service Pack 1 (versions pour systèmes Itanium comprises) ;
- Microsoft Windows Server 2003 x64 Edition.

3 Résumé

Une vulnérabilité a été identifiée dans Microsoft Agent. Une personne malveillante pourrait exploiter celle-ci afin d'exécuter des commandes arbitraires sur la machine vulnérable.

4 Description

Une vulnérabilité a été identifiée dans Microsoft Agent, un ensemble de services permettant la représentation d'agents logiciels comme des personnalités interactives. Il ne manipulerait pas correctement certains fichiers d'extension .ACF (pour *Microsoft Agent Character File*).

Une personne malveillante pourrait exploiter cette vulnérabilité en construisant une page Web particulière. La visite de cette dernière pourrait alors provoquer l'exécution de code arbitraire sur le système vulnérable. Cette attaque nécessite cependant que le navigateur accepte les contrôles ActiveX.

5 Solution

Se référer au bulletin de sécurité MS06-068 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-068 du 14 novembre 2006 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-068.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-068.msp>
- Référence CVE CVE-2006-3445 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3445>

Gestion détaillée du document

15 novembre 2006 version initiale.