

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la gestion ActiveX par l'Explorateur 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-2006-AVI-437>

Gestion du document

Référence	CERTA-2006-AVI-437
Titre	Vulnérabilité dans la gestion ActiveX par l'Explorateur Windows
Date de la première version	11 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-057 du 10 octobre 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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP Professionnel Edition x64 ;
- Microsoft Windows Server 2003 (Service Pack 1, Edition x64, Itanium).

3 Description

Une vulnérabilité a été identifiée dans l'explorateur de Microsoft Windows, quand celui-ci manipule des données issues du contrôle ActiveX `WebViewFolderIcon`, servant à l'affichage en mode Web.

Une personne malveillante pourrait construire une page Web particulière, et inciter un utilisateur à la visiter, que ce soit par son navigateur Internet Explorer, ou sous le format d'un courrier électronique en HTML. Il aurait alors le moyen d'exécuter des commandes arbitraires à distance sur le système vulnérable de l'utilisateur.

Le CERTA rappelle à cet égard qu'il est fortement recommandé de désactiver l'ActiveX par défaut sur une machine.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS06-057 du 10 octobre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-057.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-057.msp>
- Alerte technique de l'US-CERT TA06-270A du 27 septembre 2006 :
<http://www.us-cert.gov/cas/techalerts/TA06-270A.html>
- Référence CVE CVE-2006-3730 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3730>

Gestion détaillée du document

11 octobre 2006 version initiale.