

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Windows Media Encoder 9 Series

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-450>

Gestion du document

Référence	CERTA-2008-AVI-450
Titre	Vulnérabilité dans Windows Media Encoder 9 Series
Date de la première version	10 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-053 du 09 septembre 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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Packs 2 et 3 ;
- Windows XP Professionnel Edition x64, Service Pack 2 compris ;
- Windows Server 2003 Service Packs 1 et 2, y compris Edition x64 ;
- Windows Vista, Service Pack 1 et Edition x64 compris ;
- Windows Server 2008 pour systèmes 32-bit ou x64.

3 Résumé

Une vulnérabilité a été identifiée dans le contrôle ActiveX installé par Windows Media Encoder 9 Series. L'exploitation de celle-ci, par exemple via une page Web spécialement construite, peut entraîner l'exécution de code arbitraire sur un système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans le contrôle ActiveX `wmex.dll` installé par Windows Media Encoder 9 Series. Le produit n'est pas installé par défaut mais si c'est le cas, alors le contrôle ActiveX dispose des propriétés SFS (*Safe for Scripting*). Une personne malveillante peut exploiter cette vulnérabilité par le biais d'une page Web spécialement construite afin de faire exécuter du code arbitraire sur le système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS08-053 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-053 du 09 septembre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-053.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-053.msp>
- Référence CVE CVE-2008-3008 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3008>

Gestion détaillée du document

10 septembre 2008 version initiale.