

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft DirectX

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-535>

Gestion du document

Référence	CERTA-2007-AVI-535
Titre	Vulnérabilités dans Microsoft DirectX
Date de la première version	12 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-064 du 11 décembre 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

- DirectX 7.0 sur Microsoft Windows 2000 Service Pack 4 ;
- DirectX 8.1 sur Microsoft Windows 2000 Service Pack 4 ;
- DirectX 9.0c sur Microsoft Windows 2000 Service Pack 4 ;
- DirectX 9.0c sur Microsoft Windows XP Service Pack 2 ;
- DirectX 9.0c sur Windows XP Professionnel Édition x64 et Windows XP Professionnel Édition x64 Service Pack 2 ;
- DirectX 9.0c sur Windows Server 2003 Service Pack 1 et Windows Server 2003 Service Pack 2 ;
- DirectX 9.0c sur Windows Server 2003 Édition x64 et Windows Server 2003 Édition x64 Service Pack 2 ;
- DirectX 9.0c sur Windows Server 2003 avec SP1 pour les systèmes Itanium et Windows Server 2003 avec SP2 pour les systèmes Itanium ;
- DirectX 10.0 sur Windows Vista ;
- DirectX 10.0 sur Windows Vista Édition x64.

3 Résumé

Deux vulnérabilités concernant DirectX permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été identifiées dans Microsoft DirectX :

- la première faille concerne le traitement de fichiers SAMI (*Synchronized Accessible Media Interchange*) et permet l'exécution de code arbitraire à distance si un utilisateur ouvre un fichier spécialement construit ;
- la deuxième vulnérabilité est une erreur dans le traitement de fichiers WAV et AVI. Une personne malintentionnée pourrait ainsi exécuter du code arbitraire à distance en incitant un utilisateur à visiter un site web ou à ouvrir un courrier électronique spécialement conçu.

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 MS07-064 du 11 décembre 2007 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-064.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-064.msp>
- Référence CVE CVE-2007-3901
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3901>
- Référence CVE CVE-2007-3895
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3895>

Gestion détaillée du document

12 décembre 2007 version initiale.