Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 15 juillet 2009
N° CERTA-2009-ALE-009-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft DirectShow

Gestion du document

Référence	CERTA-2009-ALE-009-001
Titre	Vulnérabilité dans Microsoft DirectShow
Date de la première version	29 mai 2009
Date de la dernière version	15 juillet 2009
Source(s)	Avis de sécurité Microsoft KB971778 du 28 mai 2009
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

- Déni de service à distance ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- DirectX 7.0 pour Microsoft Windows 2000 Service Pack 4 ;
- DirectX 8.1 pour Microsoft Windows 2000 Service Pack 4 ;
- DirectX 9.0x pour Microsoft Windows 2000 Service Pack 4, Windows XP Service Pack 2 et 3 et Windows Server 2003 Service Pack 2.

3 Résumé

Une vulnérabilité a été identifiée dans la manipulation de fichiers multimédia Quicktime par Microsoft DirectShow (quartz.dll). Elle peut être exploitée à distance par le biais de pages Web spécialement construites afin d'exécuter, lors de la navigation sur ces pages, du code arbitraire sur le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans la manipulation de fichiers multimédia Quicktime par Microsoft DirectShow (quartz.dll).

Elle peut être exploitée à distance par le biais de pages Web spécialement construites afin d'exécuter, lors de la navigation sur ces pages, du code arbitraire sur le système vulnérable. L'exploitation peut se faire indépendemment du navigateur choisi dans la mesure où un module de lecture multimédia est utilisé.

La pré-visualisation ou le passage de la souris sur un fichier malveillant (répertoire de partage par exemple) peut également provoquer la compromission du système.

Des codes d'exploitation sont actuellement disponibles sur l'Internet.

5 Contournement provisoire

Le filtrage ou la désactivation de certains formats de fichiers QuickTime n'est pas suffisant. D'autres formats peuvent également contenir des données QuickTime (les `AVI` par exemple). Il faut donc désactiver de préférence l'interprétation de ces données. Cela peut se faire en supprimant la clé de registre suivante :

`HKC_ROOT\CLSID\{D51BD5A0-7548-11CF-A520-0080C77EF58A}`

L'avis de sécurité KB971778 de Microsoft pointe vers un service nommé `Fix it` permettant d'effectuer cette opération sous forme d'un logiciel à installer.

Une autre mesure peut consister à restreindre l'accès à la bibliothèque `quartz.dll`. La procédure est aussi indiquée dans l'avis de sécurité KB971778. Cette mesure peut cependant avoir des effets de bord sur certains lecteurs multimédia et des applications tierces.

6 Solution

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

7 Documentation

- Avis CERTA-2009-AVI-273 du 15 juillet 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-273/index.html
- Bulletin de sécurité Microsoft MS09-028 du 14 juillet 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-028.mspx
  http://www.microsoft.com/technet/security/bulletin/MS09-028.mspx
- Avis de sécurité Microsoft KB971778 du 28 mai 2009 :
  http://www.microsoft.com/france/technet/security/advisory/971778.mspx
  http://www.microsoft.com/technet/security/advisory/971778.mspx
  http://support.microsoft.com/kb/971778/fr/
- Bloc-Notes Microsoft SRD, "New vulnerability in quartz.dll Quicktime parsing", 28 mai 2009 :
  http://blogs.technet.com/srd/archive/2009/05/28/new-vulnerability-in-quicktime-parsing.aspx
- Bloc-notes Microsoft MSRC, "Microsoft Security Advisory 971778 Vulnerability in Microsoft DirectShow Released", 28 mai 2009 :
  http://blogs.technet.com/msrc/archive/2009/05/28/microsoft-security-advisory-971778-vulnerability-in-microsoft-directshow-released.aspx
- Référence CVE CVE-2009-1537 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1537
- Bloc-Notes Microsoft SRD, "MS08-033: So what breaks when you ACL quartz.dll?", 10 juin 2008 :
  http://blogs.technet.com/srd/archive/2008/06/10/ms08-033-so-what-breaks-when-you-acl-quartz-dll.aspx

Gestion détaillée du document

29 mai 2009 version initiale.

14 juillet 2009 ajout du lien vers le correctif.