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-010-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le contrôle ActiveX Microsoft Video

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-2009-ALE-010`

Gestion du document

Référence	CERTA-2009-ALE-010-001
Titre	Vulnérabilité dans le contrôle ActiveX Microsoft Video
Date de la première version	07 juillet 2009
Date de la dernière version	15 juillet 2009
Source(s)	Bulletin de sécurité Microsoft 972890 du 06 juillet 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows Server 2003 ;
- Microsoft Windows XP.

3 Résumé

Une vulnérabilité dans le contrôle *ActiveX* `Microsoft Video` permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une erreur dans le contrôle *ActiveX* `Microsoft Video` (*msvidctl.dll*) en charge de la gestion de flux vidéo permet à une personne distante malintentionnée d'exécuter du code arbitraire via une page web spécialement construite.

Cette vulnérabilité est déjà exploitée sur l'Internet et ne necéssite pas forcément de contenu vidéo sur la page visitée.

5 Contournement provisoire

Les moyens de contournement suivants sont disponibles :

– `Microsoft` a publié un contournement provisoire permettant de désactiver le contrôle *ActiveX* mis en cause. Une application est disponible sur le bulletin de sécurité `Microsoft` (cf. la section Documentation). Afin de désactiver le contrôle *ActiveX*, il faut placer la valeur *Compatibility Flags* pour chaque *Class Identifier* suivants comme décrit ci-dessous :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\
{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}]
"Compatibility Flags"=dword:00000400
```

Liste des *Class Identifiers* :
{011B3619-FE63-4814-8A84-15A194CE9CE3}
{0149EEDF-D08F-4142-8D73-D23903D21E90}
{0369B4E5-45B6-11D3-B650-00C04F79498E}
{0369B4E6-45B6-11D3-B650-00C04F79498E}
{055CB2D7-2969-45CD-914B-76890722F112}
{0955AC62-BF2E-4CBA-A2B9-A63F772D46CF}
{15D6504A-5494-499C-886C-973C9E53B9F1}
{1BE49F30-0E1B-11D3-9D8E-00C04F72D980}
{1C15D484-911D-11D2-B632-00C04F79498E}
{1DF7D126-4050-47F0-A7CF-4C4CA9241333}
{2C63E4EB-4CEA-41B8-919C-E947EA19A77C}
{334125C0-77E5-11D3-B653-00C04F79498E}
{37B0353C-A4C8-11D2-B634-00C04F79498E}
{37B03543-A4C8-11D2-B634-00C04F79498E}
{37B03544-A4C8-11D2-B634-00C04F79498E}
{418008F3-CF67-4668-9628-10DC52BE1D08}
{4A5869CF-929D-4040-AE03-FCAFC5B9CD42}
{577FAA18-4518-445E-8F70-1473F8CF4BA4}
{59DC47A8-116C-11D3-9D8E-00C04F72D980}
{7F9CB14D-48E4-43B6-9346-1AEBC39C64D3}
{823535A0-0318-11D3-9D8E-00C04F72D980}
{8872FF1B-98FA-4D7A-8D93-C9F1055F85BB}
{8A674B4C-1F63-11D3-B64C-00C04F79498E}
{8A674B4D-1F63-11D3-B64C-00C04F79498E}
{9CD64701-BDF3-4D14-8E03-F12983D86664}
{9E77AAC4-35E5-42A1-BDC2-8F3FF399847C}
{A1A2B1C4-0E3A-11D3-9D8E-00C04F72D980}
{A2E3074E-6C3D-11D3-B653-00C04F79498E}
{A2E30750-6C3D-11D3-B653-00C04F79498E}
{A8DCF3D5-0780-4EF4-8A83-2CFFAACB8ACE}
{AD8E510D-217F-409B-8076-29C5E73B98E8}
{B0EDF163-910A-11D2-B632-00C04F79498E}
{B64016F3-C9A2-4066-96F0-BD9563314726}
{BB530C63-D9DF-4B49-9439-63453962E598}
{C531D9FD-9685-4028-8B68-6E1232079F1E}
{C5702CCC-9B79-11D3-B654-00C04F79498E}
{C5702CCD-9B79-11D3-B654-00C04F79498E}
{C5702CCE-9B79-11D3-B654-00C04F79498E}
{C5702CCF-9B79-11D3-B654-00C04F79498E}

{C5702CD0-9B79-11D3-B654-00C04F79498E}
{C6B14B32-76AA-4A86-A7AC-5C79AAF58DA7}
{CAAFDD83-CEFC-4E3D-BA03-175F17A24F91}
{D02AAC50-027E-11D3-9D8E-00C04F72D980}
{F9769A06-7ACA-4E39-9CFB-97BB35F0E77E}
{FA7C375B-66A7-4280-879D-FD459C84BB02}
Remarque : Cette désactivation peut empêcher la visualisation de vidéos avec `Internet Explorer`.

– utiliser un navigateur alternatif.

Rappel : d'une manière générale la désactivation des contrôles *ActiveX* par défaut reste une bonne pratique.

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-278 du 15 juillet 2009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-278/index.html
– Bulletin de sécurité Microsoft MS09-032 du 14 juillet 2009 :
http://www.microsoft.com/france/technet/security/Bulletin/MS09-032.mspx
http://www.microsoft.com/technet/security/Bulletin/MS09-032.mspx
– Bulletin de sécurité Microsoft 972890 du 06 juillet 2009 :
http://support.microsoft.com/kb/972890
http://www.microsoft.com/technet/security/advisory/972890.mspx
– Lien de téléchargement du contournement provisoire Microsoft :
http://go.microsoft.com/?linkid=9672398
– Référence CVE CVE-2008-0015 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015

Gestion détaillée du document

07 juillet 2009 version initiale.
15 juillet 2009 ajout de la référence au bulletin de sécurité Microsoft MS09-032.