



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2011
N° CERTA-2011-ALE-001-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le moteur de rendu graphique de 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-2011-ALE-001>

Gestion du document

Référence	CERTA-2011-ALE-001-002
Titre	Vulnérabilité dans le moteur de rendu graphique de Windows
Date de la première version	05 janvier 2011
Date de la dernière version	10 février 2011
Source(s)	Alerte de sécurité Microsoft 2490606 du 04 janvier 2011
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

- Windows XP SP3 ;
- Windows XP Pro SP2 64bits ;
- Windows Vista SP1 et SP2 (32bits et 64bits) ;
- Windows Server 2003 SP2 (32 bits et 64 bits) ;
- Windows Server 2003 SP2 (Itanium) ;
- Windows Server 2008 (32bits et 64 bits) ;
- Windows Server 2008 (Itanium) ;
- Windows Server 2008 SP2 (32bits et 64 bits) ;
- Windows Server 2008 SP2 (Itanium).

3 Résumé

Un correctif a été publié le 08 février 2011.

Une vulnérabilité non corrigée dans le moteur de rendu graphique de Windows permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité non corrigée a été découverte dans le moteur de rendu graphique de Windows. Elle permet d'exécuter du code malveillant au moyen d'une image d'aperçu (miniature ou *thumbnail*) spécialement réalisée. Une personne malintentionnée distante peut faire exécuter du code arbitraire à une victime en la dupant et en lui faisant ouvrir un document, ou suivre un lien malveillant, entraînant la visualisation d'une miniature spécialement réalisée.

Des exemples de code d'exploitation de cette vulnérabilité sont d'ores et déjà recensés sur l'Internet.

5 Contournement provisoire

Microsoft propose comme moyen de contournement de limiter les droits sur la bibliothèque responsable du rendu graphique des miniatures, le fichier `shimgvw.dll`. Cela est faisable grâce aux commandes suivantes exécutées en tant qu'administrateur :

- Pour les systèmes Windows XP et Windows Server 2003 :

```
Echo y| cacls %WINDIR%\SYSTEM32\shimgvw.dll /E /P "Tout le monde":N
```

- pour les systèmes Windows Vista 32 bits et Windows Server 2008 32 bits :

```
takeown /f %WINDIR%\SYSTEM32\SHIMGVW.DLL
icacls %WINDIR%\SYSTEM32\SHIMGVW.DLL /save %TEMP%\SHIMGVW_ACL.TXT
icacls %WINDIR%\SYSTEM32\SHIMGVW.DLL /deny "Tout le monde":(F)
```

- pour les systèmes Windows Vista 64 bits et Windows Server 2008 64 bits :

```
takeown /f %WINDIR%\SYSTEM32\SHIMGVW.DLL
takeown /f %WINDIR%\SYSWOW64\SHIMGVW.DLL
icacls %WINDIR%\SYSTEM32\SHIMGVW.DLL /save %TEMP%\SHIMGVW_ACL32.TXT
icacls %WINDIR%\SYSWOW64\SHIMGVW.DLL /save %TEMP%\SHIMGVW_ACL64.TXT
icacls %WINDIR%\SYSTEM32\SHIMGVW.DLL /deny "Tout le monde":(F)
icacls %WINDIR%\SYSWOW64\SHIMGVW.DLL /deny "Tout le monde":(F)
```

Ce contournement aura pour effet, entre autre, de remplacer l'affichage des miniatures par l'affichage des icônes. Attention, il doit être validé avant d'être déployé en production. Le CERTA rappelle aussi qu'il est recommandé d'utiliser un compte utilisateur aux droits restreints et de respecter les bonnes pratiques en matière de sécurité.

6 Solution

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

Note : Les mesures de contournement provisoire doivent être supprimées avant l'application du correctif MS11-006.

7 Documentation

- Alerte de sécurité Microsoft 2490606 du 04 janvier 2011 :
<http://www.microsoft.com/technet/security/advisory/2490606.msp>
- Bulletin de sécurité Microsoft MS11-006 du 08 février 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-006.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-006.msp>
- Avis CERTA-2011-AVI-061 du 09 février 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-061>
- Référence CVE CVE-2010-3970 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3970>

Gestion détaillée du document

05 janvier 2011 version initiale.

09 février 2011 mise à jour des systèmes affectés et ajout de la référence au correctif.

10 février 2011 précision sur la suppression des mesures de contournement provisoires.