

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans 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-2007-ALE-002>

Gestion du document

Référence	CERTA-2007-ALE-002-001
Titre	Vulnérabilité dans Windows
Date de la première version	12 janvier 2007
Date de la dernière version	03 avril 2007
Source(s)	
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.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition.

3 Résumé

Une vulnérabilité non corrigée présente dans Windows permet à un utilisateur distant de provoquer un déni de service sur une application vulnérable.

4 Description

Une vulnérabilité de type débordement de mémoire dans Windows permet de provoquer un déni de service de toute application essayant de visualiser un fichier wmf. Il existe d'ores et déjà du code permettant l'exploitation de

cette faille et causant un déni de service sur toute application utilisant les composants de Windows qui permettent la visualisation des fichiers au format WMF.

Le CERTA n'a pour le moment pas connaissance d'éventuel code permettant l'exécution de code arbitraire à distance mais cette éventualité est envisageable.

03 avril 2007 :

Microsoft publie le bulletin de sécurité MS07-017 qui propose un correctif pour cette vulnérabilité. Ce bulletin est mentionné dans l'avis CERTA-2007-AVI-156.

5 Contournement provisoire

La vulnérabilité touchant probablement les mêmes composants que ceux décrits dans l'alerte CERTA-2005-ALE-019, les contournements y étant détaillés sont applicables dans le cas présent :

NB : le contournement provisoire cité en paragraphe 5.2 donne l'illusion de fonctionner sans les privilèges administrateur, du fait que l'utilisateur est informé du bon déroulement de la désactivation du composant `shimgvw.dll`. Cependant le composant vulnérable reste actif et par conséquent le système reste vulnérable.

5.1 Interdiction du composant `shimgvw.dll` dans la politique de sécurité

Le contournement provisoire suivant ne peut s'appliquer que dans le cas où vous disposez d'un ou plusieurs systèmes Microsoft Windows 2003 Server en tant que contrôleur de domaine.

Dans ce cas, vous pouvez appliquer une politique de sécurité interdisant l'utilisation du composant `shimgvw.dll` pour toute votre unité organisationnelle.

5.2 Désactivation du composant `shimgvw.dll`

Il apparaît que les applications faisant appel au composant `shimgvw.dll` de Microsoft Windows deviendraient vulnérables. Parmi les applications vulnérables, nous pouvons citer par exemple Mozilla Firefox, Google Desktop.

C'est pour cela que le CERTA propose un contournement provisoire plus radical que celui proposé au chapitre 5.2 en désactivant le composant `shimgvw.dll`. Cependant cela pourrait avoir des effets de bords sur des applications métiers utilisant cette `dll`.

Les composants de Microsoft Windows affectées par ce contournement provisoire seront au minimum :

- *GDI+ File Thumbnail Extractor Windows Picture and Fax Viewer ;*
- *HTML Thumbnail Extractor Windows Picture and Fax Viewer ;*
- *Shell Image Data Factory Windows Picture and Fax Viewer ;*
- *Shell Image Property Handler Windows Picture and Fax Viewer ;*
- *Shell Image Verbs Windows Picture and Fax Viewer ;*
- *Summary Info Thumbnail Handler (DOCFIELD) Windows Picture and Fax Viewer ;*

Procédures à suivre :

- Afin de désactiver le composant `shimgvw.dll` de Microsoft Windows :
 - Cliquez sur "Démarrer" puis sur "exécuter" ;
 - tapez "`regsvr32.exe -u shimgvw.dll`" puis "Entrée".
- Afin de réactiver (lorsque le correctif sera disponible) le composant `shimgvw.dll` de Microsoft Windows :
 - Cliquez sur "Démarrer" puis sur "exécuter" ;
 - tapez "`regsvr32.exe shimgvw.dll`" puis "Entrée".

Si vous ne disposez pas du fichier `regsvr32.exe`, il peut être téléchargé à partir du site de Microsoft, à l'adresse suivante :

<http://support.microsoft.com/kb/q267279/>

5.3 Contournement provisoire pour Internet Explorer

Afin de limiter l'impact d'un fichier wmf malveillant sur le système :

- bloquer l'exécution après téléchargement de fichier ayant l'extension wmf ;
 1. cliquez sur "Démarrer" puis sur "Poste de travail";
 2. dans le menu "Outils" cliquez sur "Options des dossiers";
 3. dans l'onglet "Types de fichiers", sélectionnez dans la liste WMF ;
 4. dans l'encadré "Détails concernant l'extension 'WMF'", cliquez sur "Avancé";
 5. cochez l'option "Confirmer l'ouverture après le téléchargement" puis acceptez les modifications.

Le contournement cité ci-dessus prévient le téléchargement et l'exécution automatique du fichier malveillant, toutefois l'utilisateur peut télécharger et exécuter manuellement le fichier et provoquer ainsi la compromission de son système.

5.4 Rappels de principes généraux

- Afficher les messages en texte brut dans votre client de messagerie conformément à la note de recommandation CERTA-2000-REC-001 (cf. Section Documentation) ;
- en complément, la règle générale de mise à jour régulière des anti-virus est bien entendu à respecter dans ce cas là ;
- mémento du CERTA sur les virus (cf. section Documentation) ;
- Note d'information du CERTA sur le SPAM (cf. Documentation).

6 Solution

Se reporter au bulletin de sécurité Microsoft MS07-017 pour l'application des correctifs.

7 Documentation

- Avis CERTA-2007-AVI-156 du 03 avril 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-156/>
- Bulletin de sécurité Microsoft MS07-017 du 03 avril 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-017.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-017.msp>

Gestion détaillée du document

12 janvier 2007 version initiale.

03 avril 2007 ajout de la référence au bulletin de sécurité Microsoft MS07-017.