

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation d'une vulnérabilité mal corrigée dans Microsoft 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-2005-ALE-019>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2005-ALE-019-006 |
| Titre | Exploitation d'une vulnérabilité mal corrigée dans Microsoft Windows |
| Date de la première version | 28 décembre 2005 |
| Date de la dernière version | 06 janvier 2006 |
| Source(s) | Bulletin de sécurité Microsoft #912840 du 28 décembre 2005 |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

- Exécution de code arbitraire à distance ;
- déni de service.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 & Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 & Server 2003 Service Pack 1 pour systèmes Itanium ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows 98 et 98 Second Edition ;
- Microsoft Windows Millennium Edition.

3 Résumé

Un code malveillant, d'ores et déjà utilisé sur l'Internet, exploite une vulnérabilité mal corrigée dans Microsoft Windows et permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

Ce code permet de télécharger et d'exécuter un autre code malveillant à l'insu de l'utilisateur. Selon certains éditeurs d'anti-virus, le second code téléchargé serait un cheval de Troie. Il apparaît que des messages électroniques non sollicités (spam) commencent à se propager en incitant à aller sur un site contenant des pages malicieusement construites et exploitant la vulnérabilité ou encore des messages avec une image véhiculant le code d'exploitation ("exploit"). Ces messages peuvent avoir par exemple pour caractéristiques:

- sujet : "happy new year";
- corps du texte : "picture of 2006";
- une pièce jointe contenant le code d'exploitation : "HappyNewYear.jpg".

Si cette image en pièce jointe est ouverte le code s'exécute et va chercher à télécharger un code malveillant qui peut être un cheval de Troie par exemple.

4 Description

Il apparaît que la vulnérabilité décrite dans le bulletin de sécurité du CERTA (cf. CERTA-2005-AVI-445) n'a été que partiellement ou incomplètement corrigée par le bulletin de sécurité Microsoft MS05-053 du 08 novembre 2005.

Cette vulnérabilité peut être exploitée au moyen d'un fichier wmf (Windows MetaFile) malicieusement construit. Un individu malveillant peut, au moyen d'un message électronique comprenant un tel fichier ou d'un site web malicieusement construit, exécuter du code arbitraire à distance, sur un système mis à jour, lors de l'ouverture du fichier.

Un fichier wmf malicieusement construit permet également de réaliser un déni de service sur de nombreuses autres fonctionnalités de Microsoft, notamment sur le processus `explorer.exe` lors de la prévisualisation d'un fichier wmf dans l'explorateur de fichiers. Il est à noter (cf. chapitre 5.2) que cette vulnérabilité concerne toutes les applications qui utilisent le moteur de rendu graphique de Microsoft. Le code d'exploitation ne se limite donc pas aux seules applications Microsoft comme Internet Explorer ou encore un client de messagerie comme Outlook mais concerne aussi par exemple Google Desktop.

5 Contournement provisoire

Les contournements provisoires cités en paragraphes 5.2 et 5.3 nécessitent les privilèges administrateur pour être appliqués sur le système.

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 (DOCFILE) 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

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité Microsoft MS06-001 (voir section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS06-001 du 05 janvier 2006 :
<http://www.microsoft.com/technet/security/bulletin/ms06-001.msp>
- Bulletin de sécurité Microsoft #912840 du 28 décembre 2005 :
<http://www.microsoft.com/technet/security/advisory/912840.msp>
- Bulletin de sécurité CERTA-2005-AVI-445 du 09 novembre 2005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-445/index.html>
- Note de recommandation CERTA-2000-REC-001 du 16 mai 2000 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-001/index.html>
- Mémento du CERTA sur les virus du 24 juin 2005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf>

Gestion détaillée du document

28 décembre 2005 version initiale.

28 décembre 2005 ajout des références aux publications du CERTA.

28 décembre 2005 ajout d'un contournement provisoire.

29 décembre 2005 ajout de la référence au bulletin de sécurité de Microsoft.

30 décembre 2005 ajout d'un contournement provisoire.

01 janvier 2006 ajout des caractéristiques de certains mails de spam.

06 janvier 2006 mise à jour de la section Solution, ajout de la référence vers le bulletin de sécurité MS06-001 de Microsoft.