

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité 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-2007-ALE-008>

Gestion du document

Référence	CERTA-2007-ALE-008-003
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	29 mars 2007
Date de la dernière version	03 avril 2007
Source(s)	Annnonce de sécurité sur le bloc-notes McAfee du 28 mars 2007
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

A la date de rédaction de ce bulletin d'alerte, la liste des systèmes affectés peut encore évoluer.

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP 64-bit Edition Version 2003 (Itanium) ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 pour systèmes Itanium (avec SP1 et SP2) ;
- Microsoft Windows Server 2003 Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Vista.

3 Résumé

Une vulnérabilité non corrigée présente dans Microsoft Windows ferait actuellement l'objet d'une exploitation à distance à l'aide d'un code malveillant, nommé par certains antivirus `Exploit-ANIfile.c` ou `TROJ_ANICMOO.AX`. Cette vulnérabilité serait liée à celle corrigée par Microsoft dans le bulletin de sécurité MS05-002 du 11 janvier 2005 et détaillée dans CERTA-2005-AVI-011.

4 Description

Cette vulnérabilité permettrait à un utilisateur distant malintentionné d'exécuter du code arbitraire au moyen d'un fichier de données animées (icône ou curseur) (`.ani`) spécialement construit. L'exploitation de cette vulnérabilité ne nécessite aucune interaction de la part de l'utilisateur, dans la mesure où Internet Explorer interprète ce type de fichiers sans action particulière. L'infection peut également avoir lieu par ouverture de courrier via Outlook ou par téléchargement d'un tel fichier ANI (transferts par USB par exemple). Cette vulnérabilité ne concerne pas directement Outlook et Internet Explorer, mais la bibliothèque de fonctions `user32.dll` de Microsoft Windows.

Cette vulnérabilité est massivement exploitée sur l'Internet et Microsoft a publié l'avis de sécurité 935423 à ce sujet.

03 avril 2007 :

Le CERTA a publié l'avis CERTA-2007-AVI-156, suite à la publication du bulletin de sécurité MS07-017 par Microsoft.

5 Contournement provisoire

- Filtrer les fichiers (icône ou curseur) (`.ani`) au niveau des serveurs mandataires ou locaux ;
- utiliser un navigateur Internet alternatif à Microsoft Internet Explorer ;
- configurer les clients de messagerie de manière à afficher les messages électroniques en texte brut. Cette solution est cependant imparfaite.

6 Solution

Appliquer le correctif annoncé par Microsoft dans le bulletin de sécurité MS07-017 du 03 avril 2007.

7 Documentation

- Bulletin de sécurité Microsoft MS07-017 du 03 avril 2007 :
<http://www.microsoft.com/technet/security/Bulletin/MS07-017.msp>
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-017.msp>
- Avis CERTA-2007-AVI-156 du 03 avril 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-156/>
- Avis de sécurité Microsoft 935423 du 29 mars 2007 :
<http://microsoft.com/technet/security/advisory/935423.msp>
- Annonce de sécurité sur le Web Log McAfee du 28 mars 2007 :
<http://www.avertlabs.com/research/blog/?p=230>
- Description du code malveillant "Exploit-ANIfile.c" détecté par McAfee :
http://vil.nai.com/vil/content/v_141860.htm
- Description du code malveillant "TROJ_ANICMOO.AX" détecté par Trend Micro :
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_ANICMOO.AX
- Avis CERTA CERTA-2005-AVI-011 du 12 janvier 2005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-011/index.html>
- Bulletin de sécurité Microsoft MS05-002 du 11 janvier 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-002.msp>

- Article concernant le premier ver exploitant la vulnérabilité de cet avis, ISC SANS :
<http://isc.sans.org/diary.html?storyid=2550>
- Référence CVE CVE-2007-0038 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0038>

Gestion détaillée du document

29 mars 2007 version initiale.

30 mars 2007 ajout de la référence CVE.

02 avril 2007 ajout de références concernant l'exploitation massive de la vulnérabilité.

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