

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Multiples vulnérabilités de produits Microsoft

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-2006-ALE-011>

Gestion du document

Référence	CERTA-2006-ALE-011-006
Titre	Multiples vulnérabilités de produits Microsoft
Date de la première version	31 août 2006
Date de la dernière version	11 octobre 2006
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

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

2 Systèmes affectés

- Suite bureautique Microsoft Office versions 2000SP3, 2002SP2, 2002SP3, 2003SP1, 2003SP2 ;
- Suite bureautique Mac Office versions v.X et 2004 ;
- Works versions 8.0 et 8.5 ;
- Wordpad toutes versions ;
- Internet Explorer et famille Outlook.

3 Résumé

De multiples vulnérabilités affectent certains produits de l'éditeur Microsoft. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné afin de provoquer un déni de service ou une exécution de code arbitraire à distance sur la machine cible. Des codes malveillants exploitant certaines de ces vulnérabilités sont disponibles sur l'Internet.

4 Description

- Un grand nombre de vulnérabilités révélées publiquement affectent la gamme Office. Ces vulnérabilités peuvent être exploitées par le biais de documents malicieusement contruits dont l'ouverture peut provoquer l'exécution de commandes dans le contexte utilisateur.
- Plusieurs autres vulnérabilités ont été découvertes dans des versions d'Internet Explorer. Ces vulnérabilités permettent à un attaquant de compromettre le navigateur, directement ou par le biais d'une dll vulnérable (vgx.dll). Cette bibliothèque est utilisée pour prendre en compte le format VML (Vector Markup Vector Language). Ce format fondé sur le langage XML est utilisé pour éditer certaines images. Deux vecteurs d'attaques sont possibles :
 - via une page HTML spécifiquement conçue pour exploiter la faille d'Internet Explorer ;
 - via des messages électroniques qui seraient lus à l'aide des clients de la famille d'Outlook avec prise en compte du langage HTML. Des messages malicieux se propagent déjà sur l'Internet.
- Comme cela a été déjà souligné à de nombreuses reprises par le CERTA, il est fortement recommandé de désactiver par défaut les options ActiveX et les scripts en général en choisissant éventuellement leur activation pour les sites de confiance nécessitant l'usage de tels composants ou programmes.

Un bulletin de sécurité Microsoft annonce officiellement une vulnérabilité dans MS Office Word 2000. Une référence CVE est associée à cette vulnérabilité, qui est exploitée actuellement par du code malveillant.

5 Contournement provisoire

Suite bureautique MS-Office N'ouvrir que les documents bureautiques de confiance, et utiliser une suite bureautique alternative à jour (OpenOffice, par exemple).

Internet Explorer 1 Utiliser un navigateur alternatif à jour (Mozilla, Firefox, Opéra, etc...)

Internet Explorer 2 Désactiver les options ActiveX, les scripts (cf. bulletin d'actualité du CERTA)

Internet Explorer 3 et Outlook Désactiver la bibliothèque vgx.dll :

```
regsvr32.exe "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll" -u
```

Une mise à jour de sécurité, publiée par Microsoft, est désormais disponible. Elle permet de corriger une des vulnérabilités citées dans ce bulletin d'alerte, en l'occurrence celle présente dans la bibliothèque vgx.dll. Un bulletin de sécurité du CERTA reprend cette vulnérabilité ainsi que la solution associée.

Se référer à l'avis du CERTA référencé CERTA-2006-AVI-410 du 27 septembre 2006 disponible à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-410/index.html>

6 Solution

Se référer aux bulletins de sécurité de l'éditeur pour obtenir les mises à jour (cf. Documentation).

7 Documentation

- Bulletin de sécurité Microsoft 925059 :
<http://www.microsoft.com/technet/security/advisory/925059.msp>
- Bulletin de sécurité Microsoft 925444 :
<http://www.microsoft.com/technet/security/advisory/925444.msp>
- Bulletin de sécurité Microsoft 925568 :
<http://www.microsoft.com/technet/security/advisory/925568.msp>
- Bulletin de mise à jour Microsoft MS06-055 :
<http://www.microsoft.com/technet/security/bulletin/MS06-055.msp>
- Bulletin de mise à jour Microsoft MS06-058 :
<http://www.microsoft.com/technet/security/bulletin/MS06-058.msp>
- Bulletin de mise à jour Microsoft MS06-059 :
<http://www.microsoft.com/technet/security/bulletin/MS06-059.msp>

- Bulletin de mise à jour Microsoft MS06-060 :
<http://www.microsoft.com/technet/security/bulletin/MS06-060.msp>
- Bulletin de mise à jour Microsoft MS06-062 :
<http://www.microsoft.com/technet/security/bulletin/MS06-062.msp>
- Avis du CERTA numeros CERTA-2006-AVI-410, CERTA-2006-AVI-438, CERTA-2006-AVI-439, CERTA-2006-AVI-440, CERTA-2006-AVI-442 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-410/index.html>
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-438/index.html>
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-439/index.html>
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-440/index.html>
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-442/index.html>
- Bulletin d'actualité (N°37)du CERTA :
<http://www.certa.ssi.gouv.fr/site/certa-2006-ACT-037.pdf>
- Bulletin d'actualité (N°27)du CERTA :
<http://www.certa.ssi.gouv.fr/site/certa-2006-ACT-027.pdf>
- Bulletin d'actualité (N°30)du CERTA :
<http://www.certa.ssi.gouv.fr/site/certa-2006-ACT-030.pdf>
- Référence CVE CVE-2006-4534 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4534>
- Référence CVE CVE-2006-3866 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3866>

Gestion détaillée du document

31 août 2006 Version initiale.

5 septembre 2006 Diffusion de code.

19 septembre 2006 Rappels sur les ActiveX.

20 septembre 2006 Ajouts références Microsoft et CVE.

22 septembre 2006 Ajout diffusion via la messagerie.

27 septembre 2006 Ajout de la référence à l'avis CERTA référencé CERTA-2006-AVI-410.

11 octobre 2006 Ajout de la solution et mise en forme.