

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Internet Explorer

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-2010-ALE-001>

Gestion du document

Référence	CERTA-2010-ALE-001-002
Titre	Vulnérabilité dans Microsoft Internet Explorer
Date de la première version	15 janvier 2010
Date de la dernière version	22 janvier 2010
Source(s)	Bulletin de sécurité Microsoft #979352 du 14 janvier 2010
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

- Microsoft Internet Explorer 6 ;
- Microsoft Internet Explorer 7 ;
- Microsoft Internet Explorer 8.

3 Résumé

Une vulnérabilité dans Microsoft Internet Explorer permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité due à une référence à un pointeur non valide permet à une personne malintentionnée d'exécuter du code arbitraire à distance. Des exploitations limitées de cette vulnérabilité ont déjà été constatées.

Le CERTA rappelle que les vulnérabilités d'Internet Explorer sont exploitables au moyen de documents Microsoft Office (cf. bulletin d'actualité CERTA-2009-ACT-012).

5 Contournement provisoire

Un correctif de sécurité est disponible depuis le 21 janvier 2010, se référer à l'avis CERTA-2010-AVI-025.

Dans l'attente d'un correctif de l'éditeur, le CERTA recommande l'utilisation d'un navigateur alternatif.

Le CERTA rappelle également qu'il est fortement conseillé de naviguer sur l'Internet avec un compte utilisateur aux droits limités et la désactivation de l'interprétation de code dynamique (*JavaScript*, *ActiveX*, ...). De plus, l'activation du *DEP* (*Data Execution Prevention*) peut limiter l'impact de cette vulnérabilité.

Des contournements permettent d'empêcher l'exploitation de la vulnérabilité via des documents Microsoft Office.

Dans Office 2007, il faut désactiver totalement la prise en compte des ActiveX dans les documents : dans le menu principal, sélectionner « Options Word », « Centre de gestion de la confidentialité », « Paramètres du Centre de gestion de la confidentialité », « Paramètres ActiveX », et enfin l'option « Désactiver tous les contrôles sans notification. »

Dans Office 2003, il n'est pas possible de désactiver la prise en compte des ActiveX. Toutefois, la désactivation de la prise en compte des fichiers de type XML permet de limiter l'exploitation de la vulnérabilité pour les scénarios d'exploitation découverts jusqu'à présent.

Ceci se fait en modifiant la clé de registre suivante :

```
HKCU\Software\Policies\Microsoft\Office\11.0\Word\Security\FileOpenBlock
```

et en affectant 1 à la valeur (de type DWORD) XmlFiles. Il faut faire de même pour les autres applications Microsoft Office (remplacer Word par Excel, Powerpoint, etc.).

Ce contournement pour Office 2003 peut avoir des effets de bord et doit donc être utilisé avec précaution.

6 Solution

Le bulletin de sécurité MS010-002 de Microsoft corrige le problème.

Se référer à ce bulletin pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS10-002 du 21 janvier 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-002.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-002.mspx>
- Avis CERTA-2010-AVI-025 du 22 janvier 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-025/>
- Bulletin de sécurité Microsoft #979352 du 14 janvier 2010 :
<http://www.microsoft.com/technet/security/advisory/979352.mspx>
- Bulletin d'actualité CERTA-2009-ACT-012 du 20 mars 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-012/>
- Référence CVE CVE-2010-0249 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249>

Gestion détaillée du document

15 janvier 2010 version initiale.

21 janvier 2010 modification des sections « Description » et « Contournement provisoire » pour la prise en compte des documents Office.

22 janvier 2010 ajout de la section « Solution ».