

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-2008-ALE-016>

Gestion du document

Référence	CERTA-2008-ALE-016-004
Titre	Vulnérabilité dans Microsoft Internet Explorer
Date de la première version	10 décembre 2008
Date de la dernière version	17 décembre 2008
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 à distance.

2 Systèmes affectés

- Microsoft Internet Explorer 5.01 Service Pack 4 ;
- Microsoft Internet Explorer 6 ;
- Microsoft Internet Explorer 6 Service Pack 1 ;
- Microsoft Internet Explorer 7.

3 Résumé

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

4 Description

Une vulnérabilité de type corruption de mémoire a été identifiée dans une fonction de la bibliothèque `mshtml.dll` utilisée par *Microsoft Internet Explorer*. La faille permet à une personne malintentionnée d'exécuter du code arbitraire sur le poste vulnérable d'un utilisateur en l'incitant à visiter une page Web spécialement conçue. Du code d'exploitation est disponible sur l'Internet.

5 Contournement provisoire

Le CERTA recommande les mesures suivantes :

- désactiver le Javascript par défaut et ne le réactiver qu'au cas par cas sur des sites de confiance ;
- utiliser un navigateur alternatif.

Le CERTA rappelle également qu'il est fortement conseillé de naviguer avec un compte utilisateur aux droits restreints.

D'autres contournements ont été émis par l'éditeur, notamment :

- la désactivation de la fonctionnalité *XML Island* ;
- la désinscription de `OLEDB32.DLL` ;
- la modification des ACL (*Access Control List*) de `OLEDB32.DLL` ;
- la modification des ACL d'intégrité de `OLEDB32.DLL` (sur Windows Vista) ;
- la désactivation de la fonctionnalité *Row Position* de `OLEDB32.DLL`.

Certains contournements ont plus d'effets de bord que d'autres (notamment, la désinscription ou la modification des ACL de `OLEDB32.DLL`). Se référer au bulletin de sécurité de Microsoft pour plus de détails.

Enfin, l'activation du DEP (*Data Execution Prevention*) peut rendre l'exploitation plus difficile.

6 Solution

Microsoft a émis une mise à jour hors du cycle mensuel pour corriger cette vulnérabilité. Se référer à l'avis CERTA-2008-AVI-604 pour l'obtention des correctifs.

7 Documentation

- Avis CERTA-2008-AVI-604 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-604/index.html>
- Bulletin de sécurité Microsoft 961051 du 10 décembre 2008 :
<http://www.microsoft.com/technet/security/advisory/961051.mspx>
- Référence CVE CVE-2008-4844
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4844>

Gestion détaillée du document

10 décembre 2008 version initiale.

11 décembre 2008 mise à jour du contournement et ajout de références.

12 décembre 2008 mise à jour des produits affectés et du contournement provisoire.

15 décembre 2008 mise à jour du contournement provisoire.

17 décembre 2008 ajout de la section solution.