

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2006-AVI-150>

Gestion du document

Référence	CERTA-2006-AVI-150
Titre	Multiples vulnérabilités dans Microsoft Internet Explorer
Date de la première version	12 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-013 du 11 avril 2006
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 5.0 Service Pack 4 ;
- Microsoft Internet Explorer 6 Service Pack 1 ;
- Microsoft Internet Explorer 6 pour Microsoft Windows Server 2003 ;
- Microsoft Internet Explorer 6 pour Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Internet Explorer 6 pour Microsoft Windows XP Service Pack 2.

3 Résumé

Plusieurs vulnérabilités dans Microsoft Internet Explorer laissent la possibilité à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités existent dans certaines versions du navigateur Microsoft Internet Explorer. Les plus importantes sont détaillées ci-dessous :

- l'appel de certains objets HTML (`DHTML Method Call`) peut provoquer un débordement de mémoire. Un utilisateur malveillant peut profiter de cette vulnérabilité au moyen d'une page web spécialement conçue pour exécuter du code arbitraire à distance.
- la manipulation de plusieurs événements dans un élément HTML n'est pas correctement gérée par Internet Explorer. De la même façon, un utilisateur malveillant peut utiliser ses vulnérabilités dans une page web dédiée, et ainsi exécuter du code arbitraire sur toute machine vulnérable visitant cette page.
- une application HTML (connue sous le nom de HTA) construite d'une certaine manière peut contourner le contrôle de sécurité opéré par Internet Explorer.
- l'analyse syntaxique du code HTML par Internet Explorer (`HTML Parsing`) présente plusieurs vulnérabilités permettant l'exécution de code arbitraire à distance au moyen d'une page web contenant des balises HTML non conformes.
- certaines adresses réticulaires (`URLs`) contenant des caractères particuliers à deux octets peuvent être utilisées pour exécuter du code arbitraire à distance. Cette vulnérabilité ne devrait pas concerner les versions françaises ou anglaises de Microsoft Internet Explorer.
- un utilisateur malveillant peut usurper l'adresse affichée dans le navigateur. Il peut ainsi provoquer l'affichage dans la barre d'adressage d'une adresse qui ne correspond pas au site visité. Cette technique est par exemple utilisable dans des cas de filoutage.

5 Solution

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité Microsoft MS06-013 (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-013 du 11 avril 2006 :
<http://www.microsoft.com/france/technet/securite/MS06-013.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-013.msp>
- Référence CVE CVE-2006-1359 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359>
- Référence CVE CVE-2006-1245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1245>
- Référence CVE CVE-2006-1388 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1388>
- Référence CVE CVE-2006-1185 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1185>
- Référence CVE CVE-2006-1186 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1186>
- Référence CVE CVE-2006-1188 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1188>
- Référence CVE CVE-2006-1189 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1189>
- Référence CVE CVE-2006-1190 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1190>
- Référence CVE CVE-2006-1191 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1191>
- Référence CVE CVE-2006-1192 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1192>

Gestion détaillée du document

12 avril 2006 version initiale.