

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-2008-AVI-499>

Gestion du document

Référence	CERTA-2008-AVI-499
Titre	Multiples vulnérabilités dans Microsoft Internet Explorer
Date de la première version	15 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-058 du 14 octobre 2008
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Microsoft Internet Explorer 7 et les versions antérieures.

3 Résumé

Cette mise à jour de sécurité corrige six vulnérabilités dont cinq signalées confidentiellement et une révélée publiquement. Ces vulnérabilités permettent d'exécuter du code arbitraire à distance à l'aide d'un document HTML spécifiquement écrit.

4 Description

Cette mise à jour de sécurité corrige six vulnérabilités. Les quatre premières, listées ci-dessous, permettent à un attaquant ou à un script d'accéder à une fenêtre de navigation dans un autre domaine ou une autre zone d'Internet Explorer.

- vulnérabilité inter-domaines liée à la propriété "emplacement" (*Window Location*) de la fenêtre de navigation - CVE-2008-2947;
- vulnérabilité inter-domaines liée à l'élément HTML - CVE-2008-3472;
- vulnérabilité inter-domaines liée à la gestion des événements - CVE-2008-3473;
- vulnérabilité de divulgation d'informations inter-domaines - CVE-2008-3474.

Les deux dernières, listées ci-dessous, concernent l'accès à de la mémoire ou des objets HTML non initialisés et elles permettent l'exécution de code arbitraire à distance :

- vulnérabilité de corruption de mémoire non initialisée - CVE-2008-3475;
- vulnérabilité de corruption de mémoire dans les objets HTML - CVE-2008-3476.

5 Solution

Se référer au bulletin Microsoft MS08-058 du 14 octobre 2008 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-058 du 14 octobre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-058.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-058.msp>
- Référence CVE CVE-2008-2947 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2947>
- Référence CVE CVE-2008-3472 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3472>
- Référence CVE CVE-2008-3473 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3473>
- Référence CVE CVE-2008-3474 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3474>
- Référence CVE CVE-2008-3475 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3475>
- Référence CVE CVE-2008-3476 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3476>

Gestion détaillée du document

15 octobre 2008 version initiale.