

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-AVI-481>

Gestion du document

Référence	CERTA-2010-AVI-481
Titre	Vulnérabilités dans Internet Explorer
Date de la première version	13 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-071 du 12 octobre 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Internet explorer 6.x, 7.x et 8.x.

3 Résumé

Plusieurs vulnérabilités affectent Internet Explorer permettant la divulgation de données ou l'exécution de code arbitraire à distance

4 Description

Plusieurs vulnérabilités affectent Internet Explorer :

- le mécanisme d'autocomplétion permet à un utilisateur malveillant d'accéder indûment à des données ;

- le filtrage par la fonction *toStaticHTML* permet à un utilisateur malveillant d'exécuter du code à distance avec les droits de l'utilisateur connecté ;
- le traitement de certains caractères dans les feuilles de style (CSS) permet à un utilisateur malveillant d'accéder indûment à des données ;
- le traitement d'objets non initialisés ou détruits présente un défaut permettant à un utilisateur malveillant d'exécuter du code à distance avec les droits de l'utilisateur connecté. L'une de ces vulnérabilités est liée à l'ouverture de documents HTML par Word ;
- le traitement des éléments de type *Anchor* permet à un utilisateur malveillant d'accéder indûment à des données ;
- le cloisonnement entre domaines est imparfait et permet à un utilisateur malveillant de récupérer des informations liées à la connexion de l'utilisateur sur un site d'un autre domaine.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS10-071 du 12 octobre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-071.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-071.msp>
- Référence CVE CVE-2010-0808 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0808>
- Référence CVE CVE-2010-3243 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3243>
- Référence CVE CVE-2010-3324 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3324>
- Référence CVE CVE-2010-3325 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3325>
- Référence CVE CVE-2010-3326 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3326>
- Référence CVE CVE-2010-3327 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3327>
- Référence CVE CVE-2010-3328 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3328>
- Référence CVE CVE-2010-3329 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3329>
- Référence CVE CVE-2010-3330 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3330>
- Référence CVE CVE-2010-3331 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3331>

Gestion détaillée du document

13 octobre 2010 version initiale.