

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-304>

Gestion du document

Référence	CERTA-2008-AVI-304
Titre	Vulnérabilités dans Microsoft Internet Explorer
Date de la première version	11 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-031 du 10 juin 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

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

Tous les systèmes d'exploitation Windows utilisant ces versions du navigateur sont potentiellement affectés.

3 Résumé

Des vulnérabilités ont été identifiées dans le navigateur Microsoft Internet Explorer. L'exploitation de celles-ci peuvent conduire une personne malveillante distante à récupérer des informations auxquelles elle ne devrait pas avoir accès ou à exécuter du code arbitraire sur le système vulnérable.

4 Description

Des vulnérabilités ont été identifiées dans le navigateur Microsoft Internet Explorer :

- le navigateur ne manipulerait pas correctement des appels de méthode pour des objets HTML, en particulier `substringData()` appliqué à des objets DOM spécialement construits ;
- le navigateur n'interprète pas correctement certains en-têtes de requêtes HTTP permettant à une personne distante de contourner la politique de sécurité du navigateur (*same origin policy*) via une page Web spécialement construite.

5 Solution

Se référer au bulletin de sécurité MS08-031 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-031 du 10 juin 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-031.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-031.msp>
- Bulletin de sécurité ZDI-08-039 du 10 juin 2008 :
<http://www.zerodayinitiative.com/advisories/ZDI-08-039>
- Référence CVE CVE-2008-1442 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1442>
- Référence CVE CVE-2008-1544 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1544>

Gestion détaillée du document

11 juin 2008 version initiale.