

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-545>

Gestion du document

Référence	CERTA-2006-AVI-545
Titre	Multiples vulnérabilités dans Microsoft Internet Explorer
Date de la première version	13 décembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-072 du 12 décembre 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Internet Explorer 5.01 ;
- Microsoft Internet Explorer 6.

3 Résumé

De multiples vulnérabilités présentes dans Microsoft Internet Explorer permettent l'exécution de code arbitraire à distance ou le contournement de la politique de sécurité.

4 Description

La première vulnérabilité exploite une mauvaise gestion de la libération de la mémoire dans certaines situations. Une personne malintentionnée peut utiliser cette vulnérabilité afin d'exécuter du code arbitraire à distance par le biais d'une page Web spécialement conçue.

La seconde vulnérabilité réside dans une mauvaise gestion des appels des fonctions des scripts au format DHTML. Un utilisateur malveillant peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance par le biais d'une page Web spécialement conçue.

La troisième vulnérabilité consiste en une mauvaise gestion des opérations Glisser-Déplacer (Drag and Drop) dans certaines conditions. Un utilisateur malveillant exploitant cette vulnérabilité pourrait accéder à certains fichiers présents sur l'ordinateur de sa victime.

La quatrième vulnérabilité permet de divulguer le contenu mis en cache dans le dossier Temporary Internet Files. Une personne malveillante exploitant cette vulnérabilité pourrait accéder à certains fichiers présents sur l'ordinateur de sa victime par le biais d'une page Web spécialement conçue. L'exploitation de cette vulnérabilité nécessite une action de l'utilisateur.

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 MS06-072 du 12 décembre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-072.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-072.msp>
- Référence CVE CVE-2006-5579 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5579>
- Référence CVE CVE-2006-5581 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5581>
- Référence CVE CVE-2006-5578 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5578>
- Référence CVE CVE-2006-5577 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5577>

Gestion détaillée du document

13 décembre 2006 version initiale.