Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 14 juin 2006
N° CERTA-2006-AVI-237

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Internet Explorer

Gestion du document

Référence	CERTA-2006-AVI-237
Titre	Multiples vulnérabilités dans Microsoft Internet Explorer
Date de la première version	14 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 13 juin 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

- Internet Explorer 5.0 Service Pack 4 ;
- Internet Explorer 6 Service Pack 1 ;
- Internet Explorer 6.

3 Résumé

De multiples vulnérabilités ont été identifiées dans Microsoft Internet Explorer. Celles-ci permettraient à un utilisateur malveillant d'exécuter des commandes arbitraires à distance, ou collecter des informations auxquelles il ne devrait pas accéder.

4 Description

De multiples vulnérabilités ont été identifiées dans le navigateur Microsoft Internet Explorer. Parmi celles-ci, nous notons :

- une mauvaise gestion de certaines erreurs : un utilisateur malveillant peut créer un site contenant une page particulière qui engendre volontairement une erreur. Le navigateur vulnérable des personnes visitant cette page provoque ainsi un débordement de mémoire, et l'exécution de code arbitraire sur la machine ;
- une lecture non correcte de code HTML au format `UTF-8` : de la même manière, un utilisateur malveillant peut créer un site contenant une page particulière utilisant cette vulnérabilité ;
- un contrôle défectueux de certains ActiveX concernant `DXImageTransform` : il est conseillé dans la mesure du possible de refuser les ActiveX au niveau du navigateur ;
- une usurpation possible de la barre d'adressage : un utilisateur malveillant peut construire une page particulière qui affiche une barre d'adressage issue d'un site authentique, mais dont le contenu est illégitime ;
- un enregistrement de fichiers au format *multipart HTML* (`.mht`) non correct : un utilisateur malveillant qui arrive à persuader une personne d'enregistrer une page spécialement construite sous ce format pourrait ainsi exécuter du code arbitraire sur la machine de cette personne ;
- une mauvaise manipulation des images au format ART (`.art`) : ce format est normalement utilisé par les logiciels d'AOL (*America Online*), mais Internet Explorer intègre une librairie particulière pour les afficher. Un utilisateur malveillant peut créer une page Web contenant une image ART spécialement construite, qui, une fois affichée dans le navigateur d'une personne visitant la page, entraînera l'exécution de commandes arbitraires. Un résultat identique est obtenu si l'utilisateur envoie une telle image malveillante dans un courrier électronique lu au format HTML.

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 MS06-021 du 13 juin 2006 :
  http://www.microsoft.com/france/technet/securite/MS06-021.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-021.mspx
- Bulletin de sécurité Microsoft MS06-022 du 13 juin 2006 :
  http://www.microsoft.com/france/technet/securite/MS06-022.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-022.mspx
- Référence CVE CVE-2006-2382 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2382
- Référence CVE CVE-2006-2383 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2383
- Référence CVE CVE-2006-2384 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2384
- Référence CVE CVE-2006-2385 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2385
- Référence CVE CVE-2006-2218 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2218
- Référence CVE CVE-2006-1626 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1626
- Référence CVE CVE-2006-1303 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1303
- Référence CVE CVE-2005-4089 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4089

Gestion détaillée du document

14 juin 2006 version initiale.