Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2006
N° CERTA-2006-AVI-340-002

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Multiples vulnérabilités dans Internet Explorer



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2006-AVI-340-002 |
| Titre | Multiples vulnérabilités dans Internet Explorer |
| Date de la première version | 09 août 2006 |
| Date de la dernière version | 13 septembre 2006 |
| Source(s) | Bulletin de sécurité Microsoft MS06-042 du 08 août 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 ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- Microsoft Internet Explorer 5.01 Service Pack 4 ;
- Microsoft Internet Explorer 6 (Service Pack 1 inclus).

## 3 Résumé

De multiples vulnérabilités ont été identifiées dans les versions 5.01 et 6 de Microsoft Internet Explorer. Celles-ci pourraient être exploitées par une personne malveillante afin d'obtenir des informations confidentielles, ou d'exécuter des commandes arbitraires sur le système ayant une version du navigateur vulnérable.

# 4 Description

De multiples vulnérabilités ont été identifiées dans les versions 5.01 et 6 de Microsoft Internet Explorer. Elles pourraient être exploitées par une personne malveillante afin d'obtenir des informations confidentielles, ou d'exécuter des commandes arbitraires sur le système ayant une version du navigateur vulnérable. Parmi celles-ci :

- une mauvaise manipulation des informations de style d'une page HTML, données par `CSS` (pour *Cascading Style Sheet*). Une personne malveillante peut construire une page web `HMTL` particulière : lorsque un internaute utilisant un navigateur vulnérable parcourt cette page, cela entraîne l'exécution de commandes arbitraires sur son système.
- de mauvaises interprétations d'objets `COM` utilisés par les ActiveX.
- une application non correcte des domaines de sécurité lors de l'exécution de scripts (Javascript par exemple). Ceux-ci pourraient, sous certaines conditions, accéder à des ressources locales du système ayant un navigateur vulnérable.
- une mauvaise interprétation de pages Web lorsqu'une redirection intervient, et qu'elle pointe vers une page utilisant une technique de compression (`gzip` par exemple). Ceci peut être utilisé par une personne malveillante pour obtenir des informations confidentielles sur le système ayant un navigateur vulnérable.
- une manipulation non correcte de certaines combinaisons de mise en page HTML. Celle-ci ne nécessite pas l'activation de scripts, mais ces derniers favorisent une exploitation fructueuse de la part d'une personne malveillante. Il faut que l'utilisateur visite une page Web construite de façon particulière.
- une interprétation non correcte de certains liens `ftp`. Une personne malveillante peut construire une page particulière utilisant cette vulnérabilité, avec un lien ftp donné. Il pourrait lui-même envoyer des commandes `ftp` au serveur, et donc contourner la politique de sécurité ou élever ses privilèges.

# 5 Solution

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

La première version du correctif étant vulnérable (cf alerte du CERTA du 24 août 2006), l'éditeur à mis à disposition une seconde version du correctif le 25 août 2006 et recommande d'appliquer ce correctif au plus vite.

La seconde version du correctif étant vulnérable, l'éditeur a mis à disposition une nouvelle version du correctif le 12 septembre 2006, et recommande d'appliquer ce dernier en complément des précédents.

# 6 Documentation

- Bulletin de sécurité Microsoft MS06-042 du 09 août 2006 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS06-042.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-042.mspx
- Référence CVE CVE-2006-3280 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3280
- Référence CVE CVE-2006-3450 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3450
- Référence CVE CVE-2006-3451 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3451
- Référence CVE CVE-2006-3637 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3637
- Référence CVE CVE-2006-3638 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3638
- Référence CVE CVE-2006-3639 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3639
- Référence CVE CVE-2006-3640 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3640
- Référence CVE CVE-2004-1166 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1166
- Bulletin d'alerte CERTA-2006-ALE-010 du 24 août 2006 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-010/index.html

– Bulletin de sécurité eEye EEYEB-AD20060912 du 12 septembre 2006 :
http://research.eeye.com/html/advisories/published/AD20060912.html

## Gestion détaillée du document

**09 août 2006** version initiale.
**25 août 2006** modification liée à la seconde version du correctif.
**12 septembre 2006** modification liée à la mise à jour du bulletin MS06-042.