



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 juin 2007
N° CERTA-2007-AVI-263

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2007-AVI-263>

Gestion du document

Référence	CERTA-2007-AVI-263
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	13 juin 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-033 du 12 juin 2007
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 et Internet Explorer 6 Service Pack 1 sous Windows 2000 ;
- Microsoft Internet Explorer 6 sous Windows XP et Windows Server 2003 ;
- Microsoft Internet Explorer 7 sous Windows XP, Windows Server 2003 et Windows Vista.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le navigateur Microsoft Internet Explorer. L'exploitation de l'une d'elles permettrait à une personne malveillante de tromper l'utilisateur, voire d'exécuter des commandes arbitraires sur son système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le navigateur Microsoft Internet Explorer. Parmi celles-ci :

- le navigateur ne crée pas correctement les instances de certains objets COM (*Component Object Model*) pour les utiliser comme contrôles ActiveX. Cette vulnérabilité, exploitée par le biais d'une page Web spécialement construite, permet à la personne malveillante de lancer des commandes arbitraires sur le système, avec les mêmes droits que l'utilisateur connecté. Internet Explorer 7 n'est cependant pas affecté par cette vulnérabilité ;
- le navigateur ne manipule pas correctement certaines balises de style CSS (*Cascading Style Sheets*). Une page spécialement construite pourrait donc corrompre la mémoire du système, et permettre l'exécution de code ;
- le navigateur ne gère pas correctement l'installation de plusieurs paquets linguistiques, pouvant entraîner une situation de compétition (*race condition*). Cette dernière permettrait à une personne malveillante d'exécuter du code arbitraire sur le système ;
- le navigateur chercherait à accéder à un objet qui n'a pas été initialisé, ou qui a été préalablement supprimé. Ce problème peut être exploité par une personne malveillante pour, comme les précédentes vulnérabilités, exécuter du code arbitraire sur le système vulnérable ;
- le navigateur ne gère pas correctement les modifications de la page d'annulation (*cancel page*). Une personne malveillante pourrait donc tromper l'utilisateur en lui présentant une autre page spécialement construite ;
- le navigateur ne manipule pas correctement certains objets ActiveX liés à Microsoft Speech, un moyen d'interagir avec la machine pour les applications vocales.

5 Solution

Se référer au bulletin de sécurité MS07-033 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-033 du 12 juin 2007 :
<http://www.microsoft.com/france/technet/securite/MS07-033.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-033.msp>
- Référence CVE CVE-2007-0218 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0218>
- Référence CVE CVE-2007-1499 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1499>
- Référence CVE CVE-2007-1750 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1750>
- Référence CVE CVE-2007-1751 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1751>
- Référence CVE CVE-2007-2222 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2222>
- Référence CVE CVE-2007-3027 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3027>

Gestion détaillée du document

13 juin 2007 version initiale.