

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-2004-AVI-020>

---

### Gestion du document

Référence	CERTA-2004-AVI-020
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	03 février 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-004 de Microsoft
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

Ces vulnérabilités affectent les versions d'Internet Explorer suivantes :

- Internet Explorer 6 Service Pack 1;
- Internet Explorer 6 Service Pack 1 (64-Bit Edition);
- Internet Explorer 6 for Windows Server 2003;
- Internet Explorer 6 for Windows Server 2003 (64-Bit Edition);
- Internet Explorer 6;
- Internet Explorer 5.5 Service Pack 2;
- Internet Explorer 5.01 Service Pack 2, 3 et 4.

sur les plateformes :

- Microsoft Windows NT Workstation 4.0 Service Pack 6a;

- Microsoft Windows NT Server 4.0, Service Pack 6a;
- Microsoft Windows NT Server 4.0 Terminal Server Edition et Service Pack 6;
- Microsoft Windows 2000 Service Pack 2, 3 et 4;
- Microsoft Windows XP et Service Pack 1;
- Microsoft Windows XP 64-Bit Edition et Service Pack 1;
- Microsoft Windows XP 64-Bit Edition Version 2003;
- Microsoft Windows Server 2003;
- Microsoft Windows Server 2003, 64-Bit Edition.

Les applications utilisant le moteur d'Internet Explorer (Outlook, Outlook Express, ...) de ces versions afin d'interpréter des documents au format HTML se trouvent également affectées.

### 3 Résumé

Trois nouvelles vulnérabilités ont été découvertes dans certaines versions d'Internet Explorer et font l'objet d'un correctif.

### 4 Description

- Une vulnérabilité présente dans le modèle de sécurité d'Internet Explorer (cloisonnement inter-domaines), permet à un individu mal intentionné d'exécuter du code arbitraire avec les privilèges de l'utilisateur connecté, dans un domaine différent de celui dans lequel il doit être exécuté (par exemple Local Machine Zone) à l'aide d'un e-mail au format HTML ou d'un site malicieusement constitué ;
- une vulnérabilité présente dans l'opération de "glisser-déposer" d'Internet Explorer permet dans certaines conditions l'enregistrement d'un fichier sur le système sans aucun avertissement ;
- une vulnérabilité est présente dans le traitement de certaines adresses réticulaires (URL). Cette faille peut être utilisée par un individu mal intentionné afin de créer un site malicieux et d'en masquer l'adresse réelle par une autre (cf. CERTA-2003-ALE-006).

### 5 Solution

Attention, l'installation du correctif interdit l'emploi de l'authentification de type Basic Authentication avec Internet Explorer (passage de l'identifiant et du mot de passe dans l'URL) pour les protocoles HTTP, HTTP avec SSL (HTTPS).

Appliquer le correctif suivant la plateforme et la version affectée :

- Bulletin de sécurité MS04-004 de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/MS04-004.asp>

### 6 Documentation

- Référence CVE CAN-2003-1026 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1026>
- Référence CVE CAN-2003-1027 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1027>
- Référence CVE CAN-2003-1025 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1025>

## Gestion détaillée du document

03 février 2004 version initiale.