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 octobre 2004
N° CERTA-2004-AVI-342

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Internet Explorer

Gestion du document

Référence	CERTA-2004-AVI-342
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-038 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 ;
- élévation de privilèges ;

2 Systèmes affectés

Les versions suivantes d'Internet Explorer sont affectées :

- Internet Explorer 5.01 Service Pack 3 sur la plate-forme Windows 2000 SP3 ;
- Internet Explorer 5.01 Service Pack 4 sur la plate-forme Windows 2000 SP4 ;
- Internet Explorer 5.5 Service Pack 2 sur la plate-forme Windows Me ;
- Internet Explorer 6 sur la plate-forme Windows XP ;
- Internet Explorer 6 SP 1 sur les plates-formes Windows 2000 Server SP3 et SP4, Windows XP et Windows XP SP1 ;
- Internet Explorer 6 SP 1 sur les plates-formes Windows NT 4.0 Server SP6a, Windows Server 4.0 Terminal Edition SP6, Windows 98 et SE , Windows Me ;
- Internet Explorer 6 pour Windows XP SP 1 (64-Bit Edition) ;
- Internet Explorer 6 pour Windows Server 2003 ;
- Internet Explorer 6 pour Windows Server 2003 64-Bit Edition et Windows XP 64-Bit Edition Version 2003 ;
- Internet Explorer 6 pour Windows XP SP2.

3 Description

Plusieurs vulnérabilités ont été découvertes dans certaines versions d'Internet Explorer :

- une vulnérabilité dans la gestion des fichiers CSS (Cascading Style Sheets) permet l'exécution de code arbitraire à distance via une page HTML malicieusement construite (vulnérabilité CAN-2004-0842) ;
- une vulnérabilité dans le modèle de sécurité d'Internet Explorer permet à un individu mal intentionné d'exécuter du code arbitraire dans la zone de sécurité `Local Machine` via un site malicieux (vulnérabilité CAN-2004-0727) ;
- une vulnérabilité est présente dans l'`Install Engine` qui permet l'exécution de code arbitraire à distance sur le système affecté (vulnérabilité CAN-2004-0216);
- une vulnérabilité dans la gestion des événements de la fonction `glisser et déposer` d'Internet Explorer permet à un individu mal intentionné d'élever ses privilèges via une page malicieuse au format HTML (vulnérabilité CAN-2004-0839) ;
- deux vulnérabilités permettent d'afficher une adresse (URL) incorrecte dans la barre d'adresse du navigateur (vulnérabilités CAN-2004-0844 et CAN-2004-0843) ;
- une vulnérabilité dans la gestion des scripts dans certaines balises (`image tags`) permet à un individu mal intentionné d'exécuter du code arbitraire via un site malicieux (vulnérabilité CAN-2004-0841) ;
- une vulnérabilité dans la gestion du cache pour les sites SSL (Secure Socket Layer) permet à un individu mal intentionné d'exécuter du code arbitraire (vulnérabilité CAN-2004-0845).

4 Solution

- Bulletin de sécurité Microsoft MS04-038 du 12 octobre 2004 :
  http://www.microsoft.com/technet/security/bulletin/MS04-038.mspx
- Référence CVE CAN-2004-0842 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0842
- Référence CVE CAN-2004-0727 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0727
- Référence CVE CAN-2004-0216 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0216
- Référence CVE CAN-2004-0839 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0839
- Référence CVE CAN-2004-0844 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0844
- Référence CVE CAN-2004-0843 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0843
- Référence CVE CAN-2004-0841 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0841
- Référence CVE CAN-2004-0845 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0845

5 Documentation

Gestion détaillée du document

13 octobre 2004 version initiale.