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 décembre 2005
N° CERTA-2005-AVI-489-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Internet Explorer

Gestion du document

Référence	CERTA-2005-AVI-489-001
Titre	Multiples vulnérabilités dans Internet Explorer
Date de la première version	14 décembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-054 du 13 décembre 2005
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 (incluant les systèmes Itanium) ;
- Microsoft Windows Server 2003 Service Pack 1 (incluant les systèmes Itanium) ;
- Microsoft Windows Server 2003 x64 Edition Family ;
- Microsoft Windows 98, Microsoft Windows 98 Second Edition et Microsoft Windows Millennium Edition.

3 Résumé

De nombreuses vulnérabilités découvertes dans Internet Explorer permettent à un utilisateur mal intentionné de porter atteinte à la confidentialité des données ou d'exécuter du code arbitraire à distance.

4 Description

– Une vulnérabilité dans la gestion des boîtes de dialogue de téléchargement de fichier peut être exploitée afin d'exécuter du code arbitraire à distance.

  Cette vulnérabilité est due à une erreur dans le traitement des informations qui sont transmises entre les pages web et/ou une boîte de dialogue vers une boîte de dialogue pour télécharger un fichier (CAN-2005-2829) ;

– une vulnérabilité est présente dans Internet Explorer lors d'une connexion HTTPS vers un serveur mandataire (proxy) nécessitant une authentification `basic`.

  Cette vulnérabilité permet à un utilisateur distant d'avoir connaissance des adresses réticulaires (URL) en clair malgré la connexion HTTPS (CAN-2005-2830) ;

– une vulnérabilité dans la manière dont Internet Explorer exécute des objets `COM` (Component Object Model) qui ne sont pas initialement destinés à être exécutés par Internet Explorer, permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance au moyen d'un objet `COM` malicieusement construit (CAN-2005-2831) ;

– une vulnérabilité dans le traitement des objets `DOM` (Document Object Model) permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance au moyen d'un site web malicieusement constitué (CAN-2005-1790).

  Cette vulnérabilité fait l'objet d'un bulletin d'alerte du CERTA mis à jour le 14 décembre 2005 (cf. CERTA-2005-ALE-017).

5 Contournement provisoire

Se referer au bulletin de sécurité de l'éditeur pour prendre connaissance des contournements provisoires (cf. section Documentation).

6 Solution

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

7 Documentation

– Bulletin de sécurité Microsoft MS05-054 du 13 décembre 2005 :
  http://www.microsoft.com/france/technet/securite/ms05-054.mspx
  http://www.microsoft.com/technet/security/bulletin/ms05-054.mspx
– Bulletin d'alerte du CERTA CERTA-2005-ALE-017 mis à jour le 14 décembre 2005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-ALE-017/index.html
– Référence CVE CAN-2005-2829 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829
– Référence CVE CAN-2005-2830 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2830
– Référence CVE CAN-2005-2831 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2831
– Référence CVE CAN-2005-1790 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790

Gestion détaillée du document

14 décembre 2005 version initiale.

14 décembre 2005 ajout de la référence au bulletin d'alerte CERTA-2005-ALE-017 mis à jour le 14 décembre 2005.