

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité d'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-2005-ALE-005>

Gestion du document

Référence	CERTA-2005-ALE-005-002
Titre	Vulnérabilité d'Internet Explorer
Date de la première version	02 juillet 2005
Date de la dernière version	13 juillet 2005
Source(s)	Bulletin de sécurité de Microsoft 903144 du 01 juillet 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.

2 Systèmes affectés

- Internet Explorer 5.01 Service Pack 3 sur Windows 2000 Service Pack 3 ;
- Internet Explorer 5.01 Service Pack 4 sur Windows 2000 Service Pack 4 ;
- Internet Explorer 6 Service Pack 1 sur Windows 2000 Service Pack 3 et Service Pack 4, et sur Windows XP Service Pack 1 ;
- Internet Explorer 6 sur Windows XP Service Pack 2 ;
- Internet Explorer 6 Service Pack 1 sur Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Internet Explorer 6 sur Windows Server 2003 et sur Windows Server 2003 Service Pack 1 ;
- Internet Explorer 6 sur Windows Server 2003 (systèmes Itanium), Windows Server 2003 Service Pack 1 (systèmes Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003 x64 Edition, et Windows XP Professional x64 Edition ;
- Internet Explorer 5.5 Service Pack 2 sur Windows Millenium Edition ;
- Internet Explorer 6 Service Pack 1 sur Windows 98, Windows 98 SE, et Windows Millenium Edition.

3 Résumé

Une vulnérabilité dans le composant `javaprxy.dll` permet l'exécution de code arbitraire à distance.

4 Description

Le composant `javaprxy.dll` est une interface à un débogueur de la machine virtuelle java de Microsoft. La machine virtuelle java de Microsoft n'est pas installée par défaut dans :

- Windows XP Service Pack 1a et Windows XP Service Pack 2 ;
- Windows Server 2003 et Windows Server 2003 Service Pack 1.

La présence de la machine virtuelle java de Microsoft se manifeste par la présence du fichier `javaprxy.dll` et par l'existence de la commande `jview`.

Un utilisateur mal intentionné peut, en incitant sa victime à visiter un site web malicieusement constitué, exécuter du code arbitraire à distance.

Des programmes permettant de créer automatiquement des pages web malveillantes sont disponibles sur l'Internet.

Un correctif est disponible depuis le 7 juillet 2005 sur le site de Microsoft.

5 Contournement provisoire

- Désactiver les ActiveX dans Internet Explorer ;
- désactiver `javaprxy.dll` dans le registre à l'aide de la commande : `regsvr32 /u javaprxy.dll` (ceci a un impact sur les applications qui nécessitent la machine virtuelle java de Microsoft pour fonctionner) ;
- ne naviguer que sur des sites de confiance.

6 Solution

Appliquer les mises à jour de sécurité Microsoft #KB903235 pour Internet Explorer 6 pour Windows XP SP2 et Internet Explorer 6 Service Pack 1.

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

L'avis de sécurité MS05-037 corrige cette vulnérabilité

7 Documentation

- Bulletin de sécurité de Microsoft 903144 du 01 juillet 2005 :
<http://www.microsoft.com/technet/security/advisory/903144.msp>
- Bulletin de sécurité de Microsoft MS05-037 du 12 juillet 2005:
<http://www.microsoft.com/technet/security/bulletin/MS05-037.msp>
- Mise à jour de sécurité pour Internet Explorer 6 pour Microsoft Windows XP SP2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyID=c1381768-6c6d-4568-97b1-600db8798ebf&DisplayDisplayLa>
- Mise à jour de sécurité pour Internet Explorer 6 Service Pack 1 :
<http://www.microsoft.com/downloads/details.aspx?FamilyID=2a506c16-01ef-4060-bcf8-6993c55840a9&DisplayDisplayLa>

Gestion détaillée du document

02 juillet 2005 version initiale.

07 juillet 2005 ajout d'une solution et ajout des références aux mises à jour de sécurité Microsoft.

13 juillet 2005 prise en compte du bulletin de sécurité MS05-037