

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-2004-ALE-005>

Gestion du document

Référence	CERTA-2004-ALE-005-001
Titre	Vulnérabilité d'Internet Explorer
Date de la première version	09 avril 2004
Date de la dernière version	15 avril 2004
Source(s)	Avis de sécurité AusCERT AU-2004.007
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

Toutes les versions du navigateur Microsoft Internet Explorer, indépendamment des correctifs installés.

3 Résumé

Plusieurs vulnérabilités dans Microsoft Internet Explorer permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

Une variante du virus Bugbear exploite déjà ces vulnérabilités.

4 Description

Microsoft Windows utilise des fichiers d'aide compilés de type CHM (extension .chm). Ces fichiers sont au format Microsoft ITS (Microsoft InfoTech Storage). Internet Explorer peut accéder aux composants contenus dans

les fichiers d'aide de type CHM, localement ou sur un site Internet distant (en utilisant différents protocoles tels que `ms-its`, `ms-itss` ou `mk:@MSITStore`).

Le standard MHTML (RFC 2110, MIME E-Mail Encapsulation of Aggregate Documents) définit l'inclusion de plusieurs composants d'un document HTML (code HTML, images, ...) à l'intérieur d'un message électronique au format MIME. Internet Explorer peut accéder aux objets contenus dans les documents de type MHTML en utilisant les protocoles tels que `ms-its`, `ms-itss` ou `mk:@MSITStore`. Il est de plus possible de spécifier un endroit distant pour le contenu MHTML.

Une vulnérabilité de Microsoft Internet Explorer dans la gestion des éléments MHTML et du protocole ITS (en relation avec les fichiers d'aide CHM) permet à un site Internet malveillant de forcer le téléchargement d'un fichier sur le poste de la victime et de le faire exécuter avec les droits de l'utilisateur connecté.

5 Contournement provisoire

Deux contournements provisoires sont possibles à ce jour :

- Désactiver l'interprétation des fichiers d'aide au niveau du système en dissociant l'exécutable `hh.exe` des fichiers de type `.chm`. Pour cela, changer la valeur de la clef :

```
HKEY_CLASSES_ROOT\chm.file\shell\open\command
```

avec une autre valeur (`wordpad.exe` par exemple).

- Désactiver la gestion du protocole ITS. Pour cela, il faut renommer les clefs du registre Microsoft suivantes :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler\ms-its
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler\its
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PROTOCOLS\Handler\mk
```

Note : on pourra renommer ces clefs de registre en ajoutant `-off` (`ms-its` devient `ms-its-off`).

6 Solution

Un correctif a été publié le 14 avril, voir l'avis de sécurité CERTA-2004-AVI-128 pour plus d'informations : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-128/index.html>

7 Documentation

- Avis de sécurité AusCERT AU-2004.007 du 05 avril 2004 : <http://www.auscert.org.au/3990>
- Avis de sécurité Secunia SA10523 du 02 janvier 2004 : <http://secunia.com/advisories/10523>
- Avis de sécurité de l'US-CERT VU#323070 : <http://www.kb.cert.org/vuls/id/323070>
- Avis sur W32.Bugbear.c de Symantec : <http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear.c@mm.html>
- Référence CVE CAN-2004-0380 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0380>

Gestion détaillée du document

09 avril 2004 version initiale.

15 avril 2004 ajout de la référence à l'avis CERTA-2004-AVI-128.