



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 25 août 2006
N° CERTA-2006-ALE-010-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité 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-2006-ALE-010>

Gestion du document

Référence	CERTA-2006-ALE-010-002
Titre	Vulnérabilité dans Internet Explorer
Date de la première version	23 août 2006
Date de la dernière version	25 août 2006
Source(s)	Bulletin de sécurité Microsoft 923762
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 ;
- déni de service à distance.

2 Systèmes affectés

- Internet Explorer 6 SP1 sur Windows 2000 SP4 avec le correctif référencé par le bulletin MS06-042 ;
- Internet Explorer 6 SP1 sur Windows XP SP1 avec le correctif référencé par le bulletin MS06-042.

3 Résumé

Une vulnérabilité présente sur Internet Explorer peut être exploitée par un utilisateur mal intentionné, via une page html malveillante, pour réaliser un déni de service ou exécuter du code arbitraire sur un système où se trouve le produit vulnérable.

4 Description

Dans le précédent bulletin d'actualité CERTA-2006-ACT-033 publié le 18 août, nous indiquions la possibilité de réaliser un déni de service sur Internet Explorer corrigé par le correctif référencé dans le bulletin MS06-042. Microsoft annonçait la mise à disposition d'un nouveau correctif le 22 août.

Hier, mardi 22 août, Microsoft a publié le bulletin de sécurité 923762 dans lequel l'éditeur annonce un report dans l'arrivée du correctif dû à des problèmes dans le déploiement. De plus, il apparaît que la vulnérabilité est exploitable et que des codes d'exploitations sont utilisés sur Internet.

5 Contournements provisoires

Dans l'attente du correctif, nous vous recommandons :

- de passer à la version SP2 sur Windows XP ;
- d'empêcher le navigateur de spécifier dans l'entête HTTP le champ `Accept-Encoding` (gzip, deflate, compress, etc), au moyen d'un proxy web sur la machine utilisateur, ou d'une passerelle proxy au niveau du réseau.

6 Solution

Mircosoft à mis à jour le correctif référencé par le bulletin de sécurité MS06-042 et recommande aux utilisateurs d'appliquer ce correctif.

7 Documentation

- Bulletin de sécurité 923762 de Microsoft du 22 août 2006 :
<http://www.microsoft.com/technet/security/advisory/923762.msp>
- Bulletin d'actualité CERTA-2006-ACT-033 du 18 août 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-033.pdf>
- Blog MSRC de Microsoft :
<http://blogs.technet.com/msrc/>
- Référence CVE-2006-3869 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3869>
- Bulletin de sécurité Microsoft MS06-042 du 09 août 2006 :
<http://www.microsoft.com/france/technet/security/MS06-042.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-042.msp>
- Mise à jour du bulletin de sécurité CERTA-2006-AVI-340 du 25 août 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-340/index.html>

Gestion détaillée du document

23 août 2006 version initiale.

24 août 2006 correction dans les coutournements provisoires.

25 août 2006 modification du correctif référencé par l'avis Microsoft.