Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 octobre 2001
N° CERTA-2001-AVI-116-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft 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-2001-AVI-116

Gestion du document

Référence	CERTA-2001-AVI-116-001
Titre	Vulnérabilité de Microsoft Internet Explorer
Date de la première version	16 octobre 2001
Date de la dernière version	23 octobre 2001
Source(s)	Bulletin de sécurité Microsoft MS01-051
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

- Réduction des paramètres de sécurité ;
- usurpation d'identité ;
- exécution de code arbitraire.

2 Systèmes affectés

Tous les systèmes Windows équipés d'Internet Explorer 4.01, 5.5 ou 6.

3 Résumé

Internet Explorer possède trois vulnérabilités mettant en cause la façon de traiter les URL du champ `adresse` du navigateur.

4 Description

- Sous Internet Explorer, il est possible de saisir dans l'URL l'adresse IP d'un site web sous forme décimale.
  Mais une mauvaise implémentation dans la gestion des paramètres de sécurité du logiciel entraine le traitement des adresse en décimales comme des adresses du réseau local (*Zone Locale*). Par défaut, dans les versions à jour d'Internet Explorer, les paramètres de sécurité sont plus laxistes que ceux de la *Zone Internet*.
- Il est possible d'usurper l'identité d'un utilisateur navigant sur un site web. Ceci permet à un utilisateur mal intentionné d'accéder, par des services web (webmail, etc.), à des données dont il n'est pas le propriétaitre.
- Il est possible d'ouvrir une session telnet par le biais d'un lien situé dans une page en HTML. Un utilisateur mal intentionné peut, en utilisant les paramètres passés au client telnet, créer ou écraser un fichier situé n'importe où sur le disque dur du client (NT ou 2000) s'il est équipé de SFU (*Services for Unix*), et ainsi lui faire exécuter du code arbitraire.
  Cette vulnérabilité est semblable à celle décrite dans l'avis CERTA-2001-AVI-027 et le bulletin de sécurité Microsoft : MS01-015.

5 Contournement provisoire

- Paramètrer le navigateur pour qu'il traite la *Zone Locale* comme la *Zone Internet*.
- Ne pas utiliser de logiciels clients (navigateur ou courrier électronique par exemple) depuis un serveur, ni depuis une machine contenant des données sensibles.

6 Solution

Appliquer le correctif de Microsoft :
http://www.microsoft.com/windows/ie/downloads/critical/q306121/default.asp

7 Documentation

Bulletin de sécurité Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-051.asp

Gestion détaillée du document

16 octobre 2001 version initiale

23 octobre 2001 seconde version : correction de l'URL du bulletin de sécurité Microsoft du paragraphe Documentation.