Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 février 2004
N° CERTA-2003-ALE-006-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans l'affichage des adresses réticulaires

Gestion du document

Référence	CERTA-2003-ALE-006-002
Titre	Vulnérabilité dans l'affichage des adresses réticulaires
Date de la première version	19 décembre 2003
Date de la dernière version	03 février 2004
Source(s)	–
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

Usurpation d'adresse réticulaire (URL).

2 Systèmes affectés

Toutes les versions du navigateur Internet Explorer pour Windows. D'autres navigateurs, comme Mozilla, sont partiellement affectés.

3 Résumé

Une vulnérabilité dans le navigateur Internet Explorer permet l'usurpation des adresses réticulaires (URL).

4 Description

Une fonctionnalité permet de placer un *login* et un mot de passe dans une adresse réticulaire, notamment dans le but d'utiliser le protocole `ftp`.

Par exemple :
`ftp://anonymous:monmail\%40mondomaine@ftp.site.tld`

Cette fonctionnalité est parfois détournée pour induire en erreur un internaute :
`http://www.sitelegitime.tld@www.sitepirate.tld`

L'adresse réticulaire semble pointer sur `sitelegitime.tld` alors qu'en fait il pointe sur `sitepirate.tld`. C'est visible, il suffit de chercher le symbole `@` dans l'adresse reticulaire.

Une nouvelle variante permet de camoufler le symbole `@` dans l'adresse réticulaire.

En insérant la chaîne de caractères %00 ou %01 devant le caractère `@` dans une adresse réticulaire, il est possible de masquer une partie de l'URL.

5 Contournement provisoire

- Appliquer des filtres au niveau des serveurs mandataires (proxies) afin de bloquer les adresses réticulaires contenant les chaînes %00 ou %01 ;
- pour les sites utilisant le protocole HTTPS, vérifier, comme à l'accoutumée, que le certificat correspond au site que l'on est supposé visiter ;
- il est préférable de saisir manuellement les adresses réticulaires, plutôt que de suivre un lien, en particulier pour les sites sensibles (téléprocédures, santé, banques, ...) ;
- utiliser un navigateur non vulnérable.

6 Solution

Pour Internet Explorer, l'éditeur a publié un correctif. Se référer à l'avis CERTA-2004-AVI-020.
http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-020/index.html

7 Documentation

Base de connaissances Microsoft 833786 :
http://support.microsoft.com/?id=833786

Gestion détaillée du document

19 décembre 2003 version initiale.
22 décembre 2003 ajout du rappel sur les correctifs.
03 février 2004 ajout de la référence sur l'avis CERTA-2004-AVI-020.