

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le cache d'authentification 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-2000-AVI-060>

Gestion du document

Référence	CERTA-2000-AVI-060
Titre	Vulnérabilité dans le cache d'authentification d'Internet Explorer
Date de la première version	13 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft
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'identité lors de l'accès à un site web sécurisé.

2 Systèmes affectés

La vulnérabilité touche toutes les versions d'Internet Explorer (4.x et 5.x), sauf 5.5, et est indépendante du système d'exploitation.

3 Résumé

Un utilisateur mal intentionné, peut par un procédé d'usurpation d'adresse, obtenir des données d'authentification qui ne lui appartiennent pas, alors qu'elles ont été transmises à un site en mode sécurisé (lors d'un accès par HTTPS).

4 Description

Lorsqu'un utilisateur donne un identifiant et un mot de passe pour accéder à des pages web, ces données sont conservées dans un cache par Internet Explorer, de façon à être réutilisées (lors d'autres accès au même site) durant la même session. Les données confidentielles envoyées à un site lors d'une connexion en mode sécurisé, ne devraient jamais être transmises pendant des accès en mode non-sécurisé (HTTP).

La vulnérabilité réside dans le fait qu'Internet Explorer, conservant les données confidentielles utilisées lors d'un accès en mode sécurisé, les enverra aussi en clair, automatiquement, s'il s'agit du même site, lors d'accès en mode non-sécurisé.

Un utilisateur mal intentionné qui a accès au réseau situé entre le client et le serveur sécurisé, peut, en usurpant l'adresse internet d'un autre serveur, et en envoyant au client une fausse page qui cherche à se connecter par HTTP sur le site sur lequel le client s'est déjà authentifié en mode sécurisé, lire en clair les données confidentielles conservées dans le cache, qui sont envoyées automatiquement par le navigateur.

5 Solution

Appliquer le correctif de Microsoft pour Internet Explorer :
<http://www.microsoft.com/windows/ie/download/critical/q273868.htm>

6 Documentation

- le bulletin de sécurité de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/ms00-076.asp>
- la FAQ du bulletin de sécurité :
<http://www.microsoft.com/technet/security/bulletin/fq00-076.asp>

Gestion détaillée du document

13 octobre 2000 version initiale.