

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vol de cookies sous HTTPS avec les serveurs Microsoft Internet Information Server

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-064>

Gestion du document

Référence	CERTA-2000-AVI-064
Titre	Vol de cookies sous HTTPS avec les serveurs Microsoft Internet Information Server
Date de la première version	24 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

- Vol d'informations confidentielles;
- usurpation d'identité.

2 Systèmes affectés

Internet Information Server 4.0 et 5.0

3 Résumé

Les cookies échangés lors d'une session de navigation en mode sécurisé (HTTPS) sur un site sont échangés *en clair* pendant la même session, lors d'une connexion au même site en mode normal (HTTP).

4 Description

HTTP est un protocole fonctionnant en mode déconnecté. Pour simuler une session, ou préserver des préférences enregistrées lors d'une navigation sur un site afin de les réutiliser ultérieurement, on peut utiliser des petits fichiers textes appelés « *cookies* » dans lesquels sont enregistrées des informations nécessaires à l'identification de la session entre un serveur web et un navigateur client. Les cookies permettent notamment de créer un contexte de « session » lors d'une navigation sur un site web.

Au cours d'une session de navigation en mode sécurisé, il se peut que le client et le serveur échangent des cookies chiffrés. Malheureusement les pages écrites au format .ASP gèrent mal les sessions identifiées par des cookies. Lorsqu'un utilisateur navigue en mode sécurisé sur un site, et lorsque le serveur crée une ouverture de session en envoyant des cookies chiffrés au navigateur client, si cet utilisateur est amené par la suite à naviguer sur le même site en mode normal, les mêmes cookies seront alors échangés *en clair*.

Cela permet à un utilisateur mal intentionné qui maîtrise le réseau situé entre le navigateur client et le serveur, s'il réussit à amener le client à naviguer sur le même site en mode normal, de lire les cookies et de les réutiliser, en usurpant ainsi l'identité de sa victime, sur le site sécurisé.

5 Contournement provisoire

Pour les clients : désactiver les cookies sauf dans les cas de nécessité.

6 Solution

Pour les serveurs : appliquer le correctif de Microsoft :

- Pour Internet Information 4.0 :
<http://www.microsoft.com/Downloads/Release.asp?ID=25233>
- Pour Internet Information Server 5.0 :
<http://www.microsoft.com/Downloads/Release.asp?ID=25232>

7 Documentation

- Le bulletin de sécurité Microsoft et sa FAQ :
<http://www.microsoft.com/technet/security/bulletin/ms00-080.asp>
<http://www.microsoft.com/technet/security/bulletin/fq00-080.asp>
- Une RFC concernant HTTP et les cookies :
<http://www.ietf.org/rfc/rfc2109.txt>
- La page de la CNIL concernant les cookies :
<http://www.cnil.fr/traces/comment/cooki.htm>

Gestion détaillée du document

24 octobre 2000 version initiale.