

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités lors de sessions SSL

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-006>

Gestion du document

Référence	CERTA-2000-AVI-006
Titre	Vulnérabilités lors de sessions SSL
Date de la première version	07 juin 2000
Date de la dernière version	–
Source(s)	CERT IST CERT CC

TAB. 1 – *gestion du document*

1 Risques

- Usurpation de pages web ;
- Contournement des mécanismes de sécurité.

2 Systèmes concernés

Netscape Navigator 4.x et Internet Explorer 4.x et 5.x quelque soit le système utilisé.

3 Résumé

Les sessions SSL (Secure Socket Layer) permettent d'effectuer des liaisons sécurisées. Trois vulnérabilités ont été récemment découvertes permettant de contourner ces mécanismes et dont la conséquence est de détourner les informations vers un site malveillant.

4 Description

- Première vulnérabilité (Netscape Navigator et Internet Explorer)

Après avoir vérifié la validité d'un certificat émis par un site, Netscape Navigator et Internet Explorer ouvrent une session sécurisée entre le client et le serveur. Toute autre connexion HTTPS (extension au protocole HTTP mettant en oeuvre les sessions SSL) provenant de la même adresse IP est considérée par les navigateurs comme faisant partie de la même session SSL. Ces navigateurs n'effectuent dès lors pas de nouvelles vérifications.

Un site malveillant, par « usurpation d'adresse IP » peut détourner une connexion SSL vers son site.

– Deuxième vulnérabilité (Netscape Navigator)

Durant une connexion SSL, si un certificat contenant des informations erronées parvient au navigateur Netscape, un message d'avertissement demande la confirmation de la poursuite de la navigation sur ce site. Si l'utilisateur confirme la poursuite de la navigation, tout site envoyant ce même certificat erroné ne produira plus d'avertissement.

Un site malveillant, profitant de la confiance accordée à un certificat erroné peut détourner la connexion vers son site.

– Troisième vulnérabilité (Internet Explorer)

Lorsque qu'une connexion SSL est réalisée en cliquant sur un lien associé à une image ou une frame, Internet Explorer vérifie uniquement la validité de l'autorité de certification ayant délivré le certificat. Aucune vérification n'est faite sur le contenu du certificat (date d'expiration, nom du serveur...)

Un site malveillant, par « usurpation d'adresse IP » peut détourner une connexion SSL vers son site

5 Solutions

– Première vulnérabilité

– Netscape Navigator et Communicator

Appliquer le correctif pour Netscape Navigator

http://www.iplanet.com/downloads/download/detail_128_316.html

Mettre à jour Netscape Communicator avec la version 4.73

<http://home.netscape.com/download/>

Pour linux Red Hat

– <ftp://updates.redhates.com/5.2/>

– <ftp://updates.redhates.com/6.2/>

– Internet Explorer

Mise à jour d'Internet Explorer avec la version 5.01 puis appliquer le correctif (version US uniquement)

<http://www.microsoft.com/windows/ie/download/critical/patch7.htm>

– Deuxième vulnérabilité

Il n'existe actuellement aucun correctif.

Les recommandations proposées par le Cert-CC sont:

– Valider les certificats un à un;

– Rejeter les certificats non valides.

– Troisième vulnérabilité

Mise à jour d'Internet Explorer avec la version 5.01 puis appliquer le correctif (version US uniquement)

<http://www.microsoft.com/windows/ie/download/critical/patch7.htm>

Documentation

Avis du CERT/CC CA-2000-010 du 6 juin 2000
<http://www.cert.org/advisories/CA-2000-10.html>