

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Risque d'usurpation de l'identité de Sun Microsystems

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-ALE-015>

Gestion du document

Référence	CERTA-2000-ALE-015
Titre	Risque d'usurpation de l'identité de Sun Microsystems
Date de la première version	25 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun Microsystems
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.

2 Systèmes affectés

Tous les systèmes.

3 Résumé

Sun Microsystems a annoncé que l'un de leur serveur a été compromis, on ne peut donc plus faire confiance aux certificats gérés par ce serveur.

4 Description

Les certificats sont utilisés pour créer une relation de confiance entre un client et un serveur. Ils sont par exemple vérifiés lors d'une connexion sécurisée (HTTPS) à un site, du téléchargement d'un fichier de mise à jour, ou de l'exécution d'une applique java signée.

Un des serveurs de certificat de Sun ayant été compromis, il y a des risques que ses certificats soient réutilisés par des utilisateurs mal intentionnés, ou que les machines clientes de ce serveur soient compromises lors d'échanges avec celui-ci.

Les numéros de séries de ces certificats sont les suivants :

- 3181 B12D C422 SDAC A340 CF86 2710 ABE6 pour internet explorer,
- 17:05:FB:13:A2:2F:9A:F3:C1:30:F5:62:6E:12:50:4C pour Netscape Communicator (sauf Netscape6),
- 1705FB13A22F9AF3C130F5626E12504C pour Netscape6.

5 Contournement provisoire

Afin d'éviter d'exécuter des appliquestes java signées avec un certificat volé ou provenant de la machine compromise, désactiver les java, javascripts, et ActiveX comme indiqué dans les bulletins CERTA-2000-AVI-002, CERTA-2000-ALE-001 et CERTA-2000-ALE-002, CERTA-2000-INF-002.

6 Solution

Sun recommande de supprimer de votre navigateur le certificat dont les numéros de séries correspondent à ceux des certificats délivrés par ce serveur, et de vérifier les numéros de séries des éventuels certificats lors de leur installation.

Voici quelques exemples de navigateurs :

- Pour les utilisateurs d'Internet Explorer :
Dans le menu « Outils », choisir « Options », sélectionner l'onglet « Contenu » cliquer sur le bouton « Certificats » retrouver, dans la fenêtre qui apparaît alors, un certificat nommé : « Sun Microsystems Inc. ». Cliquer sur le bouton « Voir ». Si le numéro de série est le suivant, il faut détruire l'entrée :
3181 B12D C422 SDAC A340 CF86 2710 ABE6
S'il vous est proposé d'installer un certificat :
Une fenêtre apparaît demandant si vous désirez installer le certificat en question. Pour obtenir des détails sur le certificat, cliquer sur le lien hyper-texte « Sun Microsystems Inc. » Dans la nouvelle fenêtre, choisir l'onglet « détails » et y sélectionner « l'entrée Numéro de série ». Refuser le certificat si le numéro est celui indiqué ci-dessus.
- Pour les utilisateurs de Netscape Communicator :
Dans le menu « Communicator », « Outils », « Options de sécurité ». Sélectionner l'option « java/javascripts » dans la fenêtre qui apparaît. Retrouver, dans le cadre content la liste des certificats, un certificat nommé : « Sun Microsystems Inc. ». Cliquer sur le bouton « Voir le Certificat ». Si le numéro de série est le suivant, il faut détruire l'entrée :
17:05:FB:13:A2:2F:9A:F3:C1:30:F5:62:6E:12:50:4C
S'il vous est proposé d'installer le certificat :
Une boîte d'alerte apparaît, vous demandant si vous désirez installer le certificat. Pour obtenir des détails sur le certificat, cliquer sur le bouton « certificat ». Vérifier le numéro de série indiqué dans la fenêtre qui apparaît alors. Refuser le certificat si le numéro est celui indiqué ci-dessus.
- Pour les utilisateurs de Netscape6 :
Dans le menu « tâches », « Sécurité et propriété », « Gestionnaire de sécurité », dans la fenêtre qui apparaît, onglet « certificats », retrouver un certificat nommé : « Sun Microsystems Inc. ». Si le numéro de série est le suivant, il faut détruire le certificat :
1705FB13A22F9AF3C130F5626E12504C
S'il vous est proposé de l'installer :
Une boîte d'alerte apparaît demandant si vous désirez installer le certificat. Pour en savoir plus sur le certificat, cliquer sur « Plus d'informations ». Dans la fenêtre nommé « propriétés du certificat », sélectionner « numéro de série », et vérifier ce numéro. S'il correspond à celui indiqué au dessus, le refuser.

7 Documentation

L'aide du bulletin d'alert Sun Microsystems :
http://sunsolve5.sun.com/secbull/certificate_howto.html

Gestion détaillée du document

25 octobre 2000 version initiale.