



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 janvier 2005
N° CERTA-2005-AVI-028

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Failles dans les greffons Java de Sun

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-2005-AVI-028>

Gestion du document

Référence	CERTA-2005-AVI-028
Titre	Failles dans les greffons Java de Sun
Date de la première version	24 janvier 2005
Date de la dernière version	–
Source(s)	Avis de sécurité Sun #57708
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

- Divulgence d'informations ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Tout système Windows, Linux ou Solaris avec un greffon («plug-in») Java de Sun installé dans le navigateur courant ; Java étant en version 1.4 et antérieur à la révision 1.4.2_06.

3 Résumé

Il est possible pour une applique, disponible sur un site Internet malicieux, soit d'exécuter ou d'accéder à des fichiers quelconques sur le système client, soit de corrompre le fonctionnement d'une autre applique.

4 Description

Deux failles ont été identifiées dans la gestion des appliques :

- une erreur dans l'appel à du code Javascript peut être détournée pour accéder ou exécuter des fichiers ;

- un second problème permet à une applique d'en influencer une autre afin de lui faire charger des pages web ou des fichiers.

5 Contournement provisoire

La première faille peut-être combattue en désactivant le Javascript pour le cas où cela n'aurait pas déjà été fait.

6 Solution

Se référer à l'avis de sécurité de Sun pour l'obtention et l'installation d'une version 1.4.2_06 au moins de Java (cf section Documentation).

7 Documentation

Bulletin de sécurité Sun #57708 du 19 janvier 2005 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57708-1>

Gestion détaillée du document

24 janvier 2005 version initiale.