Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 août 2000
N° CERTA-2000-AVI-034

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Faille dans le serveur Java Internet 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-2000-AVI-034

Gestion du document

Référence	CERTA-2000-AVI-034
Titre	Faille dans le serveur Internet Java de SUN
Date de la première version	23 août 2000
Date de la dernière version	–
Source(s)	Foundstone
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

Exécution de code à distance.

2 Systèmes affectés

Java Web Server de Sun Microsystems sous Solaris et Windows NT.

3 Résumé

Par le biais du module d'administration et du tableau de bord de Sun Java Web Server, un utilisateur mal intentionné peut exécuter du code arbitraire sur une machine distante.

4 Description

Le module d'administration de Sun Java Web Server est accessible par défaut sur le port 9090. Un utilisateur mal intentionné peut, par le biais d'une URL spécifique, avoir accès aux « servlets » de l'application et écrire du code Java permettant d'exécuter du code arbitraire sur la machine cible.

5 Contournement provisoire

Il est possible de contourner cette vulnérabilité en désactivant le module administration.
Dans le fichier : jws_directory/properties/server/adminserver/adminservice/rules.properties
commenter la ligne : /servlet=invoker
relancer le serveur Java.
Nota : cette modification bloque la fonctionalité du module administration.

6 Solution

Correctif pour la version 1.1.3 : Patch 3
http://java.sun.com/products/java-server/jws113patch3.html

Correctif pour la version 2.0 : Patch 3
http://java.sun.com/products/java-server/jws20patch3.html

7 Documentation

Avis de foundstone
http://www.foundstone.com/FS-082200-11-JWS.txt

Gestion détaillée du document

23 août 2000 version initiale.