Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 février 2001
N° CERTA-2001-AVI-022

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans *le Java Runtime Environment* (JRE) de Sun

Gestion du document

Référence	CERTA-2001-AVI-022
Titre	Vulnérabilité dans le *Java Runtime Environment* (JRE) de Sun
Date de la première version	27 février 2001
Date de la dernière version	–
Source(s)	Bulletins de sécurité Sun et HP
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 commandes systèmes interdites, élévation de privilèges.

2 Systèmes affectés

Indépendamment du système, les versions suivantes de SDK (*Software Development Kit*) et JRE sont vulnérables :

- Sous Windows et Solaris :
  - SDK et JRE 1.2.2_005 et précédentes ;
  - SDK et JRE 1.2.1_003 et précédentes ;
  - JDK et JRE 1.1.8_003 et précédentes ;
  - JDK et JRE 1.1.7B_005 et précédentes ;
  - JDK et JRE 1.1.6_007 et précédentes.
- Sous Solaris :
  - SDK et JRE 1.2.2_05a et précédentes ;

  - SDK et JRE 1.2.1 ;
  - JDK et JRE 1.1.8_10 et précédentes ;
  - JDK et JRE 1.1.7B ;
  - JDK et JRE 1.1.6.

- Sous Linux : SDK et JRE 1.2.2_005 et précédentes.
- Sous HP MPE/iX versions 5.5, 6.0 et 6.5 :

  - JDK/JRE 1.1 ;
  - JDK/JRE 1.2 ;
  - MPE Versions A.22.04 et supérieures.

3 Résumé

Une vulnérabilité du *Java Runtime Environment* permet à un utilisateur mal intentionné d'exécuter des commandes qui lui sont normalement interdites à l'aide d'une classe Java.

4 Description

Une classe java habilement construite peut faire appel à des commandes non autorisées du système. Cependant, il faut pour cela que la permission ait été donnée à Java d'exécuter au moins une commande.

5 Contournement provisoire

Retirer à Java la permission d'exécuter des commandes en attendant d'appliquer le correctif.

6 Solution

Appliquer le correctif en fonction du produit :

- SDK et JRE 1.2.2_007 :
  http://java.sun.com/products/jdk/1.2/
- SDK et JRE 1.2.1_004
  http://java.sun.com/products/jdk/1.2.1/
- SDK et JRE 1.1.8_006
  http://java.sun.com/products/jdk/1.1/
- SDK et JRE 1.1.7B_007
  http://java.sun.com/products/jdk/1.1.7B/
- SDK et JRE 1.1.6_009
  http://java.sun.com/products/jdk/1.1.6/
- JDK et JRE 1.2.2_007 :
  http://www.sun.com/software/solaris/java/download.html
- JDK et JRE 1.1.8_12 Pour Solaris :
  http://www.sun.com/software/solaris/java/archive.html
- Pour HP MPE/iX 5.5 rechercher le correctif MPELX89D à l'adresse suivante :
  http://itrc.hp.com/
- Pour HP MPE/iX 6.0 rechercher le correctif MPELX89E à l'adresse suivante :
  http://itrc.hp.com/
- Pour HP MPE/iX 6.5 rechercher le correctif MPELX89F à l'adresse suivante :
  http://itrc.hp.com/

7 Documentation

Bulletin de sécurité Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/201&type=0&nav=sec.sba
Bulletin de sécurité HP :
http://itrc.hp.com/

Gestion détaillée du document

27 février 2001 version initiale.