Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 janvier 2003
N° CERTA-2003-AVI-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des interpréteurs XML sous de multiples systèmes et applications

Gestion du document

Référence	CERTA-2003-AVI-006
Titre	Vulnérabilité des interpréteurs XML sous de multiples systèmes et applications
Date de la première version	16 janvier 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #49922 de Sun Bulletin de sécurité #MPSB02-14
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

Déni de service.

2 Systèmes affectés

- Les applications utilisant JRun 4.0 ;
- les applications ColdFusion MX (éditions Professional, Enterprise, J2EE jusqu'aux versions d'octobre 2002) ;
- les applications Sun ONE Integration Server EAI Edition 3.0 et Unified Development Server 5.0.

3 Résumé

Il est possible d'utiliser la `DTD` (*Data Type Definition*) d'un document XML pour effectuer un déni de service local ou distant sur certaines applications utilisant un interpréteur XML.

4 Description

La DTD est la définition des structures et des balises utilisées dans un document XML.

L'interpréteur XML est utilisé dans la plupart des applications de développement de sites web, et sur de multiples serveurs HTTP.

Un utilisateur mal intentionné peut effectuer un déni de service localement ou à distance sur des applications JRun, ColdFusion et SunOne WebServer, au moyen d'une DTD habilement construite dans un document XML.

5 Solution

Consulter les bulletins de sécurité #23599 de Macromédia et #49922 de Sun (voir paragraphe Documentation) pour connaître les disponibilité des correctifs pour les applications affectées.

6 Documentation

- Bulletin de sécurité #23599 de Macromedia :
  http://www.macromedia.com/v1/handlers/index.cfm?ID=23599
- Bulletin d'alerte #49922 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F49922

Gestion détaillée du document

16 janvier 2003 version initiale.