Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2010
N° CERTA-2010-AVI-387

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Apache Geronimo

Gestion du document

Référence	CERTA-2010-AVI-387
Titre	Vulnérabilités dans Apache Geronimo
Date de la première version	17 août 2010
Date de la dernière version	–
Source(s)	Notes de version de Geronimo 2.1.6
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 arbitraire à distance ;
- déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Serveur *Apache Geronimo* versions 2.1.5 et inférieures.

3 Résumé

Des vulnérabilités concernant les composants d'*Apache Geronimo* permettent notamment à un utilisateur malveillant d'exécuter du code arbitraire à distance et de réaliser un déni de service.

4 Description

- Une vulnérabilité (CVE-2010-1622) dans le composant *SpringSource Spring Framework* permet à un attaquant d'exécuter du code arbitraire via une requête *HTTP* contenant l'adresse d'un fichier *jar* ;

– une erreur dans la gestion des *DTD* inclus dans les messages *SOAP* engendre une vulnérabilité dans le composant *Apache Axis2* (CVE-2010-1632) et *Apache CXF* (CVE-2010-2076). Elle permet à un utilisateur malveillant de déclencher des requêtes *HTTP* à des serveurs de l'intranet, de lire des fichiers arbitraires, et causer un déni de service par consommation excessive de ressources système.

5 Solution

La version 2.1.6 de *Apache Geronimo* contient les versions corrigées de ces différents modules.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité Apache Geronimo :
http://geronimo.apache.org/21x-security-report.html
– Référence CVE CVE-2010-1622 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1622
– Référence CVE CVE-2010-1632 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1632
– Référence CVE CVE-2010-2076 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2076

Gestion détaillée du document

17 août 2010 version initiale.