



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2007
N° CERTA-2007-AVI-421

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Websphere

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-2007-AVI-421>

Gestion du document

Référence	CERTA-2007-AVI-421
Titre	Multiples vulnérabilités de WebSphere
Date de la première version	28 septembre 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité d'IBM
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 ;
- injection de code indirecte (*cross site scripting*) ;
- déni de service à distance.

2 Systèmes affectés

- IBM WebSphere Application Server 6.1.x ;
- IBM HTTP Server 6.1.x.

3 Résumé

Plusieurs vulnérabilités des serveurs IBM HTTP et WebSphere permettent à un utilisateur malveillant de réaliser un déni de service, local ou à distance, ou de réaliser de l'injection de code indirecte.

4 Description

Plusieurs vulnérabilités affectent les produits IBM WebSphere :

- une erreur dans la gestion du jeu de caractères utilisé est présente dans le module *mod_status* . Elle permet à un utilisateur malveillant de réaliser, dans des circonstances particulières, de l'injection de code indirecte ;
- une erreur de traitement par le module *mod_cache* des requêtes malformées permet à un utilisateur malveillant de réaliser un déni de service à distance, dans certaines circonstances ;
- un manque de vérification de la nature des processus fils du serveur web permet à un utilisateur malveillant local de réaliser un déni de service ;
- une erreur du module *mod_proxy* permet à un utilisateur malintentionné de provoquer un arrêt inopiné (*crash*) du serveur, à distance.

5 Solution

Le correctif APAR PK52702 corrige ces problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité IBM swg1PK49295 du 16 août 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK49295>
- Bulletin de sécurité IBM swg1PK49355 du 16 août 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK49355>
- Bulletin de sécurité IBM swg1PK50467 du 04 septembre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK50467>
- Bulletin de sécurité IBM swg1PK50469 du 04 septembre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK50469>
- Bulletin de sécurité IBM swg1PK52702 du 26 septembre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702>
- Référence CVE CVE-2006-5752 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5752>
- Référence CVE CVE-2007-1863 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1863>
- Référence CVE CVE-2007-3304 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3304>
- Référence CVE CVE-2007-3847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3847>

Gestion détaillée du document

28 septembre 2007 version initiale.