



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 décembre 2007
N° CERTA-2007-AVI-560

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de serveur HTTP d'IBM

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-560>

Gestion du document

Référence	CERTA-2007-AVI-560
Titre	Vulnérabilités de serveur HTTP d'IBM
Date de la première version	24 décembre 2007
Date de la dernière version	–
Source(s)	CVE-2007-5000 CVE-2007-6203
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

Injection de code indirecte (*cross site scripting*).

2 Systèmes affectés

IBM HTTP Server.

3 Résumé

Deux vulnérabilités dans IBM HTTP Server permettent à un utilisateur malintentionné de réaliser de l'injection de code indirecte.

4 Description

Une première vulnérabilité est présente dans le module *mod_imap*. Un défaut de filtrage des données entrées permet à un utilisateur malintentionné de réaliser de l'injection de code indirecte.

Une deuxième vulnérabilité est présente dans le traitement de certaines erreurs HTTP (code HTTP 4xx). Un défaut de filtrage des données entrées permet à un utilisateur malintentionné de réaliser de l'injection de code indirecte.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité IBM swg1PK57952 du 20 décembre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK57952>
- Bulletin de sécurité IBM swg1PK58024 du 20 décembre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024>
- Référence CVE CVE-2007-5000 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5000>
- Référence CVE CVE-2007-6203 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6203>

Gestion détaillée du document

24 décembre 2007 version initiale.