

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le 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-2010-AVI-211>

Gestion du document

Référence	CERTA-2010-AVI-211
Titre	Vulnérabilités dans le serveur HTTP d'IBM
Date de la première version	14 mai 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg1PM10658 du 10 mai 2010
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

IBM HTTP Server 2.x.

3 Résumé

IBM publie un correctif cumulatif remédiant à des vulnérabilités de son serveur HTTP dont les plus graves permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités sont corrigées dans le correctif cumulatif. Elles permettaient à un utilisateur malveillant de réaliser :

- de l'exécution de code arbitraire à distance ;
- un déni de service à distance ;
- un contournement de la politique de sécurité ;
- une atteinte à la confidentialité des données ;
- une élévation de privilèges ;
- de l'injection de code indirecte à distance.

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 swg1PM10658 du 10 mai 2010 :
<http://www-01.ibm.com/support/docview.wss?uid=swg1PM10658>
- Référence CVE CVE-2008-0005 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0005>
- Référence CVE CVE-2008-2364 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2364>
- Référence CVE CVE-2008-2939 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2939>
- Référence CVE CVE-2009-0023 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0023>
- Référence CVE CVE-2009-1891 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1891>
- Référence CVE CVE-2009-1955 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1955>
- Référence CVE CVE-2009-1956 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1956>
- Référence CVE CVE-2009-2412 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2412>
- Référence CVE CVE-2009-3094 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3094>
- Référence CVE CVE-2009-3095 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3095>
- Référence CVE CVE-2009-3555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>
- Référence CVE CVE-2010-0425 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0425>
- Référence CVE CVE-2010-0434 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0434>

Gestion détaillée du document

14 mai 2010 version initiale.