

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Horde IMP

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-131>

Gestion du document

Référence	CERTA-2007-AVI-131
Titre	Vulnérabilité dans Horde IMP
Date de la première version	16 mars 2007
Date de la dernière version	–
Source(s)	Mise à jour de Horde IMP 4.1.4
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 indirecte.

2 Systèmes affectés

Horde IMP versions antérieures à 4.1.4.

3 Résumé

Deux vulnérabilités dans Horde IMP permettent à une personne malintentionnée d'effectuer des attaques de type exécution indirecte de code (*cross-site scripting*).

4 Description

Deux vulnérabilités ont été identifiées dans Horde IMP. Celles-ci concernent les fichiers `thread.php` et `search.php` qui ne contrôlent pas correctement certains paramètres, ce qui permet à un attaquant d'effectuer une attaque de type exécution de code indirecte.

5 Solution

Ces vulnérabilités sont corrigées dans la version 4.1.4 de Horde IMP (cf. section Documentation).

6 Documentation

- Annonce de sécurité de Horde IMP du 14 mars 2007 :
<http://lists.horde.org/archives/announce/2007/000316.html>

Gestion détaillée du document

16 mars 2007 version initiale.