



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mars 2007
N° CERTA-2007-AVI-132

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Horde Application Framework

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-132>

Gestion du document

Référence	CERTA-2007-AVI-132
Titre	Vulnérabilités dans Horde Application Framework
Date de la première version	16 mars 2007
Date de la dernière version	–
Source(s)	Mise à jour 3.1.4 de Horde
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

- Atteinte à l'intégrité des données ;
- Exécution indirecte de code.

2 Systèmes affectés

Horde Application Framework versions antérieures à 3.1.4.

3 Résumé

Deux vulnérabilités dans Horde permettent à un attaquant de porter atteinte à l'intégralité des données et d'effectuer une exécution indirecte de code.

4 Description

Deux vulnérabilités de Horde ont été identifiées. La première concerne une erreur des scripts `cron` et permet à une personne locale d'effacer des fichiers arbitraires. La deuxième vulnérabilité est un mauvais contrôle de paramètre lors de la sélection de langue, qui peut être exploité pour effectuer une attaque de type exécution de code indirecte (XSS).

5 Solution

La version 3.1.4 de Horde corrige ces problèmes (cf. section Documentation).

6 Documentation

- Mise à jour de Horde 3.1.4 du 14 mars 2007 :
<http://lists.horde.org/archives/announce/2007/000315.html>

Gestion détaillée du document

16 mars 2007 version initiale.