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 janvier 2009
N° CERTA-2009-AVI-036

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Horde

Gestion du document

Référence	CERTA-2009-AVI-036
Titre	Vulnérabilités dans Horde
Date de la première version	28 janvier 2009
Date de la dernière version	–
Source(s)	Annonces de sécurité de la liste 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

- Contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

- Horde versions antérieures à 3.2.4 ;
- Horde versions antérieures à 3.3.3 ;
- Horde Groupware versions antérieures à 1.1.5.

3 Résumé

Des vulnérabilités dans `Horde` permettent à une personne malintentionnée d'effectuer une injection de code indirecte (*cross-site scripting*) et de contourner la politique de sécurité.

4 Description

Des vulnérabilités ont été corrigées dans `Horde`. Celles-ci concernent un manque de contrôle de paramètres en entrée pour les fichiers `cloud_search.php` et `Image.php`. Ceci peut être exploité pour effectuer une injection de code indirecte et inclure des fichiers locaux.

5 Solution

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

6 Documentation

- Annonce de sécurité du 27 janvier 2009 pour Horde 3.2.4 :
  http://lists.horde.org/archives/announce/2009/000483.html
- Annonce de sécurité du 27 janvier 2009 pour Horde 3.3.3 :
  http://lists.horde.org/archives/announce/2009/000482.html
- Annonce de sécurité du 27 janvier 2009 pour Horde 1.1.5 :
  http://lists.horde.org/archives/announce/2009/000486.html

Gestion détaillée du document

28 janvier 2009 version initiale.