

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Horde

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-2008-AVI-121>

Gestion du document

Référence	CERTA-2008-AVI-121
Titre	Vulnérabilité dans Horde
Date de la première version	11 mars 2008
Date de la dernière version	–
Source(s)	Annonces Horde du 07 et 08 mars 2008
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 ;
- élévation de privilèges.

2 Systèmes affectés

- *Horde Application Framework* versions 3.1.6 et antérieures ;
- *Horde Groupware* versions 1.0.4 et antérieures ;
- *Horde Groupware Webmail Edition* versions 1.0.5 et antérieures.

3 Résumé

Une vulnérabilité dans *Horde* permet à un utilisateur authentifié d'inclure un fichier à distance et de l'exécuter.

4 Description

Une vulnérabilité a été découverte dans le traitement du paramètre `theme` dans *Horde*. Un utilisateur authentifié mal intentionné peut, par le biais d'une requête `POST` spécifiquement construite, inclure un fichier à distance et le faire exécuter.

5 Solution

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

6 Documentation

- Correctif pour *Horde Application Framework* :
<http://lists.horde.org/archives/announce/2008/000382.html>
- Correctif pour *Horde Groupware* :
<http://lists.horde.org/archives/announce/2008/000383.html>
- Correctif pour *Horde Groupware Webmail Edition* :
<http://lists.horde.org/archives/announce/2008/000384.html>

Gestion détaillée du document

11 mars 2008 version initiale.