

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans les produits 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-2012-AVI-302>

---

### Gestion du document

Référence	CERTA-2012-AVI-302
Titre	Vulnérabilités dans les produits Horde
Date de la première version	01 juin 2012
Date de la dernière version	–
Source(s)	Note de version Horde 772 et 773 du 29 mai 2012
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

Injection de code indirecte à distance.

## 2 Systèmes affectés

- Horde Groupware versions 4.0.7 et antérieures ;
- Horde Groupware Webmail versions 4.0.7 et antérieures.

## 3 Résumé

De multiples vulnérabilités de type XSS (*injection de code indirecte à distance*) ont été corrigées dans Horde Groupware. Ces vulnérabilités, présentes dans les fonctionnalités de messagerie et de calendrier, permettent à un utilisateur malintentionné d'exécuter du code dans le navigateur Web du client.

## 4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les versions 4.0.8 corrigent le problème.

## **5 Documentation**

- Notes de version Horde 772 et 773 du 29 mai 2012 :  
<http://lists.horde.org/archives/announce/2012/000772.html>  
<http://lists.horde.org/archives/announce/2012/000773.html>

### **Gestion détaillée du document**

**01 juin 2012** version initiale.