



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 septembre 2008  
N° CERTA-2008-AVI-458

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-458>

---

### Gestion du document

Référence	CERTA-2008-AVI-458
Titre	Multiples vulnérabilités dans Horde
Date de la première version	15 septembre 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité 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

Injection de code indirecte (*cross-site scripting*).

## 2 Systèmes affectés

- Horde Groupware versions 1.0.6 et antérieures ;
- Horde Groupware versions 1.1.2 et antérieures ;
- Horde Groupware Webmail Edition versions 1.0.7 et antérieures ;
- Horde Groupware Webmail Edition versions 1.1.2 et antérieures ;
- Horde Application Framework versions 3.1.8 et antérieures ;
- Horde Application Framework versions 3.2.2 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités sont présentes dans les produits Horde et permettent à un utilisateur distant malintentionné de réaliser des attaques de type « injection de code indirecte » (*cross-site scripting*).

## 4 Description

Deux vulnérabilités sont présentes dans plusieurs produits Horde comme Groupeware, Groupeware Webmail Edition et Application Framework. Ces vulnérabilités sont relatives à la mise en œuvre d'extensions MIME ou bien à la gestion de certains caractères d'échappement. Elles permettent à un utilisateur distant malintentionné de réaliser des attaques de type « injection de code indirecte » (*cross-site scripting*).

## 5 Contournement provisoire

## 6 Solution

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

## 7 Documentation

- Bulletins de sécurité Horde :
  - <http://marc.info/?l=horde-announce&m=122105459907561&w=2>
  - <http://marc.info/?l=horde-announce&m=122105049900311&w=2>
  - <http://marc.info/?l=horde-announce&m=122104360019867&w=2>
  - <http://marc.info/?l=horde-announce&m=122104782527315&w=2>
  - <http://marc.info/?l=horde-announce&m=122104642924629&w=2>
  - <http://marc.info/?l=horde-announce&m=122103888111491&w=2>
- Bulletin de sécurité de l'oCERT :
  - <http://www.ocert.org/advisories/ocert-2008-012.html>
- Référence CVE CVE-2008-3823 :
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3823>
- Référence CVE CVE-2008-3824 :
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3824>

## Gestion détaillée du document

15 septembre 2008 version initiale.