



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 décembre 2009
N° CERTA-2009-AVI-552-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans des 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-2009-AVI-552>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2009-AVI-552-001 |
| Titre | Vulnérabilité dans des produits Horde |
| Date de la première version | 17 décembre 2009 |
| Date de la dernière version | 24 décembre 2009 |
| Source(s) | Notes de changements des produits Horde du 15 décembre 2009 |
| 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.

2 Systèmes affectés

Les versions antérieures à :

- Horde Application Framework 3.3.6 ;
- Horde Groupware 1.2.5 ;
- Horde Groupware Webmail Edition 1.2.4.

3 Résumé

Une vulnérabilité permettant l'injection de code indirecte dans des produits Horde a été corrigée.

4 Description

Une vulnérabilité concernant les scripts d'administration de certains produits Horde et permettant à une personne malveillante distante de réaliser une injection de code indirecte au moyen d'une requête spécifiquement écrite à été corrigée.

5 Solution

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

6 Documentation

- Notes de changements des produits Horde du 15 décembre 2009 :
<http://cvs.horde.org/diff.php/horde/docs/CHANGES?r1=1.512.2.559&r2=1.512.2.589&ty=h>
<http://cvs.horde.org/diff.php/groupware/docs/groupware/CHANGES?r1=1.38.2.7&r2=1.38.2.9&ty=h>
<http://cvs.horde.org/diff.php/groupware/docs/webmail/CHANGES?r1=1.35.2.8&r2=1.32.2.9&ty=h>
- Référence CVE CVE-2009-3701 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3701>
- Référence CVE CVE-2009-4363 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4363>

Gestion détaillée du document

17 décembre 2009 version initiale.

24 décembre 2009 ajout des références CVE.