Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 février 2008
N° CERTA-2008-AVI-032-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Horde3

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-032

Gestion du document

Référence	CERTA-2008-AVI-032-001
Titre	Vulnérabilité de Horde3
Date de la première version	21 janvier 2008
Date de la dernière version	13 février 2008
Source(s)	
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- IMP Webmail 4.1.5 ;
- Horde Application Framework 3.1.5 ;
- Horde Groupware Webmail Edition 1.0.3.

3 Résumé

Une vulnérabilité de Horde permet d'exécuter du code abitraire à distance, de contourner la politique de sécurité ou de porter atteinte à l'intégrité des données.

4 Description

Le filtre HTML ne filtre pas les éléments de type <Frame> et <Frameset>. De plus, certains utilisateurs peuvent adresser des requêtes via HTTP, sans vérification de validité. Cela peut servir à effacer des messages et à les purger de la corbeille. L'exploitation de cette vulnérabilité exige l'ouverture du message malveillant par la victime.

5 Solution

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

6 Documentation

- Site de téléchargement du projet Horde :
  http://ftp.horde.org/pub/horde/horde-3.1.6.tar.gz
  http://ftp.horde.org/pub/horde/patches/patch-horde-3.1.5-3.1.6.gz
- Bulletin de sécurité Debian DSA-1470-1 du 20 janvier 2008 :
  http://lists.debian.org/debian-security-announce/debian-security-announce-2008/msg00030.html
- Bulletin de sécurité Gentoo GLSA 200802-03 du 11 février 2008 :
  http://www.gentoo.org/security/en/glsa/glsa-200802-03.xml
- Référence CVE CVE-2007-6018 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6018

Gestion détaillée du document

21 janvier 2008 version initiale ;
13 février 2008 ajout des références aux bulletins de sécurité Debian et Gentoo.