Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 décembre 2006
N° CERTA-2006-AVI-519

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Kronolith

Gestion du document

Référence	CERTA-2006-AVI-519
Titre	Vulnérabilité de Kronolith
Date de la première version	01 décembre 2006
Date de la dernière version	–
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

- Contournement de la politique de sécurité ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- *Kronolith H3* versions 2.1.3 et précédentes

3 Résumé

Horde regroupe des des applications web développées en PHP et orientées vers le travail collaboratif. *Kronolith* est le nom du gestionnaire d'agenda, *IMP* celui du serveur IMAP/webmail. La vulnérabilité permet à l'attaquant d'exécuter un code arbitraire à distance.

4 Description

Une erreur de conception de *Kronolith* permet à un utilisateur authentifié du webmail d'exécuter un code arbitraire à distance.

L'exécution de code se fait dans le contexte du serveur web.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention de la version 2.1.4 (cf. section Documentation).

6 Documentation

- Bulletin de sécurité du projet Horde du 29 novembre 2006 :
  http://lists.horde.org/archives/announce/2006/000307.html
- Bulletin de sécurité iDefense du 29 novembre 2006 :
  http://www.idefense.com/application/poi/display?id=445

Gestion détaillée du document

01 décembre 2006 version initiale.