

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Horde Application Framework 3

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-2006-AVI-366>

Gestion du document

Référence	CERTA-2006-AVI-366-001
Titre	Multiples vulnérabilités dans Horde Application Framework 3
Date de la première version	21 août 2006
Date de la dernière version	–
Source(s)	Bulletins de sécurité Horde #291 et #292 du 17 août 2006
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

Cross-Site Scripting.

2 Systèmes affectés

- Horde Application Framework versions 3.0.11 et antérieures ;
- Horde Application Framework versions 3.1.2 et antérieures.

3 Résumé

De multiples vulnérabilités dans Horde Application Framework 3 permettent à un utilisateur distant mal intentionné de réaliser une attaque de type Cross-Site Scripting.

4 Description

Deux erreurs ont été identifiées dans le fichier `index.php` de Horde Application Framework 3. Un manque de contrôle sur les paramètres passés à ce fichier permet à un utilisateur distant mal intentionné d'injecter une page web ou du script arbitraire dans le contexte du navigateur de la victime consultant le site vulnérable.

5 Solution

Les versions 3.0.12 et 3.1.3 de Horde Application Framework corrigent le problème :
<http://ftp.horde.org/pub/horde/horde-3.0.12.tar.gz>
<http://ftp.horde.org/pub/horde/horde-3.1.3.tar.gz>

6 Documentation

- Bulletin de sécurité Horde #291 concernant la version 3.0.12 :
<http://lists.horde.org/archives/announce/2006/000291.html>
- Bulletin de sécurité Horde #292 concernant la version 3.1.3 :
<http://lists.horde.org/archives/announce/2006/000292.html>
- Bulletin de sécurité FreeBSD du 17 août 2006 :
<http://www.vuxml.org/freebsd/index.html>

Gestion détaillée du document

18 août 2006 version initiale.