Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 novembre 2006
N° CERTA-2006-AVI-481-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PHP

Gestion du document

Référence	CERTA-2006-AVI-481-001
Titre	Vulnérabilité dans PHP
Date de la première version	09 novembre 2006
Date de la dernière version	17 novembre 2006
Source(s)	Bulletin de sécurité Mandriva MDKSA-2006:196 du 2 novembre 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Toutes versions antérieures à PHP 4.4.4 ;
- toutes versions antérieures à PHP 5.2.0.

3 Résumé

Une vulnérabilité découverte dans le language de script PHP permet à un utilisateur distant malintentionné d'exécuter du code arbitraire ou de provoquer un déni de service à distance.

4 Description

PHP (pour PHP Hypertext Preprocessor) est un language de script largement utilisé dans la réalisation de pages web dynamiques.

Une vulnérabilité de type débordement de mémoire a été découverte dans les fonctions `htmlentities()` et `htmlspecialchars()` peut être exploitée par un utilisateur distant malintentionné afin d'exécuter du code arbitraire ou de provoquer un déni de service sur le système vulnérable. L'exécution de code n'est possible que si le jeu de caractère `UTF-8` est selectionné.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1206 du 06 novembre 2006 :
  http://www.debian.org/security/2006/dsa-1206
- Bulletin de sécurité Mandriva MDKSA-2006:196 du 02 novembre 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:196
- Bulletin de sécurité RedHat RHSA-20006:0730 du 06 novembre 2006 :
  http://rhn.redhat.com/errata/RHSA-20006:0730.html
- Bulletin de sécurité Ubuntu USN-375-1 du 02 novembre 2006 :
  http://www.ubuntulinux.org/usn/usn-375-1
- Bulletin de sécurité Suse SUSE-SA:2006:067 du 15 novembre 2006 :
  http://www.novell.com/linux/security/advisories/2006_67_php.html
- Référence CVE CVE-2006-5465 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5465
- Référence CVE CVE-2006-5706 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5706

Gestion détaillée du document

09 novembre 2006 version initiale ;
17 novembre 2006 ajout de la référence du bulletin de sécurité Suse.