Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 janvier 2001
N° CERTA-2001-AVI-011

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de MySQL 3.23.31 et du module PHP d'Apache sous Linux

Gestion du document

Référence	CERTA-2001-AVI-011
Titre	Vulnérabilités de MySQL 3.23.31 et du module PHP d'apache sous Linux
Date de la première version	31 janvier 2001
Date de la dernière version	–
Source(s)	Avis de sécurité RedHat et Mandrake
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

- Déni de service ;
- accès en lecture à des données non-autorisées.

2 Systèmes affectés

- Linux-Mandrake 7.2
- Debian 2.2 (Potato)
- RedHat 5.2, 6.0, 6.1, 6.2, 7.0
- Linux Conectiva
- Linux Caldera
- Cette liste n'est pas exhaustive, contactez votre éditeur Linux pour savoir si votre version peut-être vulnérable.

3 Résumé

Le module PHP version 3.0.17 et 4.0.0 à 4.0.4 d'apache contient de multiples vulnérabilités, certaines étant liées à MySQL d'autres non, dans différentes éditions de Linux..

4 Description

- Une vulnérabilité concerne le module PHP 3.0.17 sous Linux RedHat.
  Elle permet à un utilisateur mal intentionné d'arrêter le service web de sa victime, à l'aide d'une requête de formulaire habilement construite.
- Le cumul de PHP et MySQL dans le même paquetage implique un cumul de vulnérabilités :

  1. Plusieurs vulnérabilités de MySQL 3.23.31 permettent à un utilisateur mal intentionné d'effectuer un dépassement de mémoire sur le serveur, d'obtenir les informations de protections des données (mots de passe hachés). De plus les fonctions de journalisation ne fonctionnent pas correctement.
  2. Une autre concerne tous les module PHP4 de la version 4.0.0 à 4.0.4 sous RedHat également.
     Il s'agit d'une erreur qui s'est glissée lors du développement du correctif concernant MySQL 3.23.31.

  Il faut donc appliquer le correctif de PHP après celui de MySQL.
- Sous Linux-Mandrake, deux problèmes de sécurité sont à corriger :

  - Un utilisateur mal intentionné peut outrepasser les directives associées à un répertoire en falsifiant une requête HTTP.
  - Il est aussi possible de mettre le « moteur PHP » `en fonction` ou `hors fonction` à distance. Ce qui permet d'obtenir les sources de n'importe quelle page web PHP même située sur un site virtuel hébergé par le serveur vulnérable.

5 Solution

Appliquer les correctifs de l'éditeur :

- Linux Mandrake
  http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-014-1.php3
- Debian 2.2 (Potato)
  http://www.debian.org/security/2001/dsa-013
- Linux Conectiva
  http://www.distro.conectiva.com.br/actualizacoes/?id=a&anuncio=000375
- RedHat
  http://www.red-hat.com/mailing-lists/redhat-announce-list/msg00218.html
  http://www.red-hat.com/mailing-lists/redhat-announce-list/msg00217.html
- Linux Caldera
  http://www.calderasystems.com/support/security/advisories/CSSA-2001-0060.txt

6 Documentation

- Documentation Mandrake :
  http://www.linux-mandrake.com/en/security/2001/mdk72-updates.php3
- Documentation Security-Focus
  http://www.securityfocus.com/bid/2205

Gestion détaillée du document

31 janvier 2001 version initiale.