Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2006
N° CERTA-2006-AVI-222-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de cURL

Gestion du document

Référence	CERTA-2006-AVI-222-001
Titre	Vulnérabilités de cURL
Date de la première version	29 mai 2006
Date de la dernière version	28 septembre 2006
Source(s)	Mise à jour du projet cURL
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.

2 Systèmes affectés

- Les versions PHP 4.4.2 et antérieures ;
- les versions PHP 5.1.4 et celles antérieures.

3 Résumé

Des vulnérabilités identifiées dans cURL (les fonctions cURL sont dans la bibliothèque `libcurl` pour PHP) peuvent être exploitées par un utilisateur local malveillant, afin de contourner la politique de sécurité associée à PHP.

4 Description

PHP est un langage de programmation pour la création de pages Internet. Il peut être configuré en `Safe Mode` afin de préciser certaines règles de sécurité (vérifier l'identifiant `UID` du propriétaire, restreindre la modification des

variables d'environnement, exécuter des programmes, etc). cURL est un moyen pour se connecter et communiquer avec un ensemble varié de serveurs (FTP, FTPS, HTTP, HTTPS, TELNET, etc). Il se présente sous la forme d'une bibliothèque nommée `libcurl` pour PHP.

Des vulnérabilités identifiées dans cURL peuvent être exploitées par un utilisateur local malveillant, afin de contourner certaines restrictions définies par `Safe Mode`.

5 Solution

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

6 Documentation

- Site du projet cURL :
  http://curl.haxx.se/
- Site décrivant `Safe Mode` pour PHP :
  http://fr2.php.net/features.safe-mode
- Mise à jour de la bibliothèque `libcurl` pour PHP :
  http://cvs.php.net/viewcvs.cgi/php-src/ext/curl/
- Bulletin de sécurité SuSE SUSE-SA:2006:052 du 21 septembre 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Sep/0006.html
- Bulletin de sécurité Ubuntu USN-320-1 du 19 juillet 2006 :
  http://www.ubuntu.com/usn/usn-320-1
- Bulletin de sécurité Ubuntu USN-320-2 du 26 juillet 2006 :
  http://www.ubuntu.com/usn/usn-320-2
- Bulletin de sécurité Mandriva MDKSA-2006:122 du 13 juillet 2006 :
  http://wwW.mandriva.com/security/advisories?name=MDKSA-2006:122
- Référence CVE CVE-2006-2563 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2563

Gestion détaillée du document

29 mai 2006 version initiale.
28 septembre 2006 ajout des références aux bulletins de sécurité SuSE, Ubuntu et Mandriva.