Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 décembre 2005
N° CERTA-2005-AVI-407-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libcURL

Gestion du document

Référence	CERTA-2005-AVI-407-003
Titre	Vulnérabilité dans la bibliothèque libcURL
Date de la première version	14 octobre 2005
Date de la dernière version	13 décembre 2005
Source(s)	Bulletin de sécurité cURL du 13 octobre 2005
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.

2 Systèmes affectés

- cURL 7.x ;
- GNU wget 1.x.

Toutes les applications utilisant la bibliothèque `libcURL` sont vulnérables.

3 Résumé

Une vulnérabilité dans la bibliothèque `libcURL` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

La bibliothèque `libcURL` comporte de nombreuses fonctions permettant le transfert de fichiers en utilisant des syntaxes de type adresses réticulaires (`URL`).

La vulnérabilité se situe dans la mise en ouvre du protocole `NTLM` de Microsoft.
Cette vulnérabilité de type débordement de mémoire est due à une erreur dans la fonction `ntlm_output` et peut être exploitée au moyen d'une requête `HTTP` malicieusement constituée.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de l'éditeur :
  http://curl.haxx.se/
- Bulletin de sécurité cURL du 13 octobre 2005 :
  http://curl.haxx.se/mail/lib-2005-10/0061.html
- Mise à jour de sécurité pour cURL en version 7.15.0 :
  http://curl.haxx.se/download.html
- Mise à jour de sécurité pour wget en version 1.10.2 :
  http://ftp.gnu.org/pub/gnu/wget/
- Bulletin de sécurité iDEFENSE #322 du 13 octobre 2005 :
  http://www.idefense.com/application/poi/display?id=322&vulnerabilities
- Bulletin de sécurité Mandriva MDKSA-2005:182 du 13 octobre 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:182
- Bulletin de sécurité Ubuntu USN-205-1 du 14 octobre 2005 :
  http://www.ubuntu.com/usn/usn-205-1/
- Bulletin de sécurité Gentoo GLSA 200510-19 du 22 octobre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200510-19.xml
- Bulletin de sécurité RedHat RHSA-2005:807 du 02 novembre 2005 :
  https://rhn.redhat.com/errata/RHSA-2005-807.html
- Bulletin de sécurité RedHat RHSA-2005:812 du 02 novembre 2005 :
  https://rhn.redhat.com/errata/RHSA-2005-812.html
- Bulletin de sécurité Debian DSA-919 du 12 décembre 2005 :
  http://www.debian.org/security/2005/dsa-919
- Référence CVE CAN-2005-3185 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3185

Gestion détaillée du document

14 octobre 2005 version initiale ;
19 octobre 2005 ajout de la référence au bulletin de sécurité Ubuntu.
21 novembre 2005 ajout des références aux bulletins de sécurités Gentoo et RedHat.
13 décembre 2005 ajout des références aux bulletins de sécurité Debian DSA-919 et RedHat RHSA-2005:812.