

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU wget

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-2005-AVI-207>

Gestion du document

Référence	CERTA-2005-AVI-207-001
Titre	Vulnérabilité de GNU wget
Date de la première version	13 juin 2005
Date de la dernière version	29 septembre 2005
Source(s)	Bulletin de sécurité Mandriva MDKSA-2005:098 du 09 juin 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

- Corruption de données ;
- exécution de code arbitraire.

2 Systèmes affectés

Toutes les versions de GNU wget des branches 1.8 et 1.9.

3 Résumé

Deux vulnérabilités dans GNU wget permettent à un utilisateur mal intentionné de corrompre des données ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

Wget est un logiciel très utilisé pour automatiser le téléchargement de fichiers distants via les protocoles HTTP et FTP.

Lors du traitement de redirection HTTP, wget effectue une mauvaise vérification de l'URL. Il est ainsi possible,

pour un administrateur mal intentionné, de créer un site HTTP malicieux, permettant de porter atteinte à l'intégrité des données ou d'exécuter du code arbitraire sur la plate-forme vulnérable.

5 Solution

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

6 Documentation

- Site Internet de GNU wget :
<http://www.gnu.org/software/wget/wget.html>
- Bulletin de sécurité Mandriva MDKSA-2005:098 du 09 juin 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:098>
- Références CVE CAN-2004-1487 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1487>
- Références CVE CAN-2004-1488 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1488>
- Bulletin de sécurité Red Hat :
<http://rhn.redhat.com/errata/RHSA-2005-771.html>

Gestion détaillée du document

13 juin 2005 version initiale.

29 septembre 2005 Bulletin Red Hat.