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 2002
N° CERTA-2002-AVI-263-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de wget

Gestion du document

Référence	CERTA-2002-AVI-263-001
Titre	Vulnérabilité de wget
Date de la première version	12 décembre 2002
Date de la dernière version	13 décembre 2002
Source(s)	Bulletin de sécurité RHSA-2002:229 de Redhat Bulletin de sécurité MDKSA-2002:086 de 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;
- corruption de données.

2 Systèmes affectés

Les versions de wget antérieures ou égales à la version 1.8.2 sont vulnérables.

3 Résumé

Une vulnérabilité présente dans wget permet à un utilisateur mal intentionné d'écraser des fichiers présents sur le poste de l'utilisateur.

4 Description

Wget est un logiciel très utilisé pour automatiser le téléchargement de fichiers distants via les protocoles `http` et `ftp`.

Lors du téléchargement de fichiers, wget ne s'assure pas que les noms des fichiers ne contiennent pas les caractères "`..`" ou ne commencent pas par "`/`".

Il est ainsi possible, pour un administrateur mal intentionné, de créer des sites FTP avec des noms de fichiers choisis de telle façon que, lors du téléchargement, ces fichiers viennent à écraser des fichiers appartenant à l'utilisateur.

5 Solution

Il est conseillé d'appliquer les correctifs des différents éditeurs (cf. section Documentation).

6 Documentation

- Site de le Free Software Foundation :
  http://www.gnu.org/software/wget/wget.html
- Bulletin de sécurité RHSA-2002:229 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2002-229.html
- Bulletin de sécurité MDKSA-2002:086 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:086
- Bulletin de sécurité DSA-209 de Debian :
  http://www.debian.org/decurity/2002/dsa-209
- Note VU#210148 du CERT/CC :
  http://www.kb.cert.org/vuls/id/210148
- Message "Directory Traversal Vulnerabilities in FTP Clients" de Steven M. Christey :
  http://lists.insecure.org/lists/vulnwatch/2002/Oct-Dec/0080.html

Gestion détaillée du document

12 décembre 2002 version initiale.
13 décembre 2002 ajout référence à l'avis DSA-209 de Debian.