Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2002
N° CERTA-2002-AVI-043-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur squid

Gestion du document

Référence	CERTA-2002-AVI-043-001
Titre	Multiples Vulnérabilités sur squid
Date de la première version	22 février 2002
Date de la dernière version	07 mars 2002
Source(s)	Bulletin de sécurité de squid
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;
- exécution d'un code arbitraire.

2 Systèmes affectés

`squid` versions 2.4.3 et antérieures.

3 Résumé

Deux vulnérabilités présentes dans `squid` permettent à un utilisateur mal intentionné de provoquer un déni de service du serveur mandataire (« proxy ») `squid`, ainsi que l'éxécution de code arbitraire.

4 Description

`squid` est un serveur mandataire très utilisé sur les plateformes Unix.

– Une vulnérabilité de type « débordement de mémoire » présente dans l'interface SNMP de `squid` permet à un utilisateur mal intentionné d'envoyer des paquets sur le port SNMP de `squid` afin de réaliser un déni de service du serveur mandataire. Ceci n'est réalisable que si l'interface SNMP est active (Désactivée par défaut).

– Une vulnérabilité de type « débordement de mémoire » présente dans la gestion des URL de type « (`ftp://`) » permet à un utilisateur mal intentionné de réaliser un déni de service du serveur mandataire ou éventuellement l'éxécution d'un code arbitraire.

– Une vulnérabilité est présente sur la désactivation de l'interface `HTCP` de `squid` (interface utilisée pour la communication d'un serveur `squid` avec les caches des serveurs `squid` distants). L'interface `HTCP` est souvent désactivée lors de l'installation de `squid` cependant quelques revendeurs active cette interface lors de l'installation de `squid`.

5 Contournement provisoire

Désactiver l'interface SNMP de `squid`.
Verifier que l'interface HTCP n'est pas installée par défaut sur votre système, au quel cas il serait préférable de réinstaller la Squid.

6 Solution

Mettre à jour `squid` avec la version `squid-2.4.4`.

7 Documentation

Bulletin de sécurité Squid-2002:1 de Squid :
http://www.squid-cache.org/Advisories/SQUID-2002_1.txt
Bulletin de sécurité FreeBSD-SA-02:12 de FreeBSD :
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:12.squid.asc
Bulletin de sécurité SUSE-SA:2002:008 de Suse :
http://www.suse.com/us/support/security

Gestion détaillée du document

22 février 2002 version initiale.
07 mars 2002 ajout référence avis SuSE.