



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 19 juillet 2002  
N° CERTA-2002-AVI-142-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité sur Squid

---

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-2002-AVI-142>

---

### Gestion du document

Référence	CERTA-2002-AVI-142-001
Titre	Vulnérabilité sur Squid
Date de la première version	05 juillet 2002
Date de la dernière version	19 juillet 2002
Source(s)	Avis de sécurité SQUID-2002:3 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

- Exécution de code arbitraire ;
- déni de service ;
- perte de confidentialité.

## 2 Systèmes affectés

Versions de squid 2.4.6 et antérieures.

## 3 Résumé

De multiples vulnérabilités présentes dans le proxy squid permettent, sous certaines conditions, à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, de réaliser un déni de service ou encore de voler des informations sur la machine cible.

## 4 Description

Plusieurs vulnérabilités présentes dans la gestion du protocole `gopher` et une vulnérabilité dans l'analyse grammaticale (parsing) des répertoires `ftp` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de l'utilisateur `squid`.

Une vulnérabilité présente dans la recherche des adresses IP dans les connexions `ftp` et une vulnérabilité présente sur les informations d'authentification des utilisateurs permettent à un utilisateur mal intentionné de voler les informations de sessions des utilisateurs authentifiés.

Une autre vulnérabilité de type « débordement de mémoire » présente dans l'authentification MSNT sur les plateformes `Windows/NT` permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'utilisateur `squid`.

## 5 Solution

Installer le correctif ou la nouvelle version 2.4.7 de `squid` correspondant à votre système (se référer à la section documentation).

## 6 Documentation

- Mise à jour de la version 2.4.6 :  
<http://www.squid-cache.org/Versions/v2/2.4/diff-2.4.STABLE6-2.4.STABLE7.gz>
- Version 2.4.STABLE7 :  
<http://www.squid-cache.org/Versions/v2/2.4/diff-2.4.STABLE7-src.tar.gz>
- Avis de sécurité SQUID-2002:3 de squid :  
[http://www.squid-cache.org/Advisories/SQUID-2002\\_3.txt](http://www.squid-cache.org/Advisories/SQUID-2002_3.txt)
- Avis de sécurité RHSA-2002:051-16 de redhat :  
<http://rhn.redhat.com/errata/RHSA-2002-051.html>
- Avis de sécurité MDKSA-2002:044 de mandrake :  
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-044.php>
- Avis de sécurité SuSE-SA:2002:025 de suze :  
[http://www.suse.com/de/support/security/2002\\_025\\_squid\\_txt.html](http://www.suse.com/de/support/security/2002_025_squid_txt.html)

## Gestion détaillée du document

**05 juillet 2002** version initiale ;

**19 juillet 2002** ajout des bulletins redhat, mandrake et suze.