

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2010-AVI-404>

---

### Gestion du document

Référence	CERTA-2010-AVI-404
Titre	Vulnérabilité dans Squid
Date de la première version	25 août 2010
Date de la dernière version	–
Source(s)	Bulletin des changements de la version Squid 3.1.7 du 24 août 2010
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 à distance.

## 2 Systèmes affectés

Squid version 3.1.6.  
Des versions antérieures peuvent être concernées.

## 3 Résumé

Une vulnérabilité dans Squid permet à un utilisateur malveillant de provoquer un déni de service à distance.

## 4 Description

Lorsqu'aucun résolveur DNS pour IPv6 n'est présent dans le serveur Squid, des réponses DNS de grande taille peuvent provoquer un déni de service.

## **5 Solution**

La version 3.1.7 remédie à ce problème.

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

## **6 Documentation**

– Bulletin des changements de la version Squid 3.1.7 du 24 août 2010 :

[http://www.squid-cache.org/Versions/v3/3.1/changesets/SQUID\\_3\\_1\\_7.html](http://www.squid-cache.org/Versions/v3/3.1/changesets/SQUID_3_1_7.html)

## **Gestion détaillée du document**

**25 août 2010** version initiale.