

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-2007-AVI-520>

---

### Gestion du document

Référence	CERTA-2007-AVI-520-001
Titre	Vulnérabilité de Squid
Date de la première version	05 décembre 2007
Date de la dernière version	14 octobre 2008
Source(s)	Bulletin de sécurité Squid SQUID-2007:2 du 27 novembre 2007
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, versions antérieures à la 2.6.STABLE18.

## 3 Résumé

Squid est affecté par une vulnérabilité permettant de réaliser un déni de service à distance.

## 4 Description

Squid est un serveur mandataire (*proxy*). Il est vulnérable à un défaut de contrôle des bornes lors de la mise à jour de son cache. Cette vulnérabilité permet à un utilisateur mal intentionné de provoquer un déni de service du serveur mandataire (CVE-2007-6239).

Le correctif initial était lui-même vulnérable à une attaque en déni de service (CVE-2008-1612).

## 5 Solution

La version 2.6.STABLE18 corrige le problème.

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

## 6 Documentation

- Bulletin de sécurité Squid SQUID-2007:2 du 27 novembre 2007 :  
[http://www.squid-cache.org/Advisories/SQUID-2007\\_2.txt](http://www.squid-cache.org/Advisories/SQUID-2007_2.txt)
- Bulletin de sécurité Debian DSA 1646 du 07 octobre 2008 :  
<http://www.debian.org/security/2008/dsa-1646>
- Bulletin de sécurité Fedora FEDORA-2008-2740 du 29 avril 2008 :  
<https://www.redhat.com/archives/fedora-package-announce/2008-April/msg00560.html>
- Bulletin de sécurité Mandriva MDVSA-2008:134 du 04 juillet 2008 :  
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité RedHat RHSA-2008:0214 du 08 avril 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0214.html>
- Bulletin de sécurité Ubuntu USN-601-1 du 14 avril 2008 :  
<http://www.ubuntulinux.org/usn/usn-601-1>
- Alerte de Secunia numéro 27910 du 04 décembre 2007 :  
<http://secunia.com/advisories/27910/>
- Référence CVE CVE-2007-6239 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6239>
- Référence CVE CVE-2008-1612 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1612>

## Gestion détaillée du document

**05 décembre 2007** version initiale.

**14 octobre 2008** Modification des versions affectées, ajout des CVE et des correctifs des distributions Linux.