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 septembre 2005
N° CERTA-2005-AVI-337-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2005-AVI-337`

Gestion du document

Référence	CERTA-2005-AVI-337-004
Titre	Multiples vulnérabilités dans Squid
Date de la première version	07 septembre 2005
Date de la dernière version	03 octobre 2005
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.

2 Systèmes affectés

Squid version 2.5.STABLE10 et versions antérieures.

3 Résumé

Deux vulnérabilités pouvant provoquer un déni de service ont été découvertes dans Squid.

4 Description

Squid est un logiciel sous licence libre servant de `Proxy cache`. Deux vulnérabilités ont été découvertes dans ce logiciel.

La première vulnérabilité est due à une erreur présente dans la fonction `sslConnectTimeout()`. Cette fonction ne gère pas correctement certaines requêtes malformées.

La seconde vulnérabilité est due à une erreur présente dans la fonction `storeBuffer()`. Là aussi, cette fonction peut être exploitée par le biais d'une requête malformée.

L'exploitation d'une de ces deux vulnérabilités peut entraîner un déni de service.

5 Solution

Appliquer les correctifs respectifs. Ces correctifs peuvent être fournis par la distribution utilisée (cf. Documentation), ou directement sur le site de l'éditeur :

- Correctif de la fonction `sslConnectTimeout()` :
  http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-sslConnectTimeout.patch
- Correctif de la fonction `storeBuffer()` :
  http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-STORE_PENDING.patch

6 Documentation

- Site de l'éditeur :
  http://www.squid-cache.org
- Bulletin de mises à jour Squid :
  http://www.squid-cache.org/Versions/v2/2.5/bugs/
- Bulletin de sécurité FreeBSD :
  http://www.vuxml.org/freebsd/pkg-squid.html
- Mises à jour Fedora :
  - Fedora Core 3 :
    http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3
  - Fedora Core 4 :
    http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4
- Bulletin de sécurité Gentoo GLSA 200509-06 du 07 septembre 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200509-06.xml
- Bulletin de sécurité Mandriva MDKSA-2005:162 du 12 septembre 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:162
- Bulletin de sécurité Debian DSA-809 du 13 septembre 2005 :
  http://www.debian.org/security/2005/dsa-809
- Bulletin de sécurité RedHat RHSA-2005:766 du 15 septembre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-766.html
- Bulletin de sécurité Suse :
  http://lists.suse.com/archive/suse-security-announce/2005-Sep/0012.html
- Référence CVE CAN-2005-2794 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2794
- Référence CVE CAN-2005-2796 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2796

Gestion détaillée du document

07 septembre 2005 version initiale.

09 sptembre 2005 ajout de la référence Gentoo.

15 septembre 2005 ajout des références Mandriva, Debian et CVE.

22 septembre 2005 ajout de la référence au bulletin de sécurité RedHat.

03 octobre 2005 ajout de la référence au bulletin de sécurité Suse.