Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2005
N° CERTA-2005-AVI-042-005

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-042

Gestion du document

Référence	CERTA-2005-AVI-042-005
Titre	Multiples vulnérabilités dans Squid
Date de la première version	01 février 2005
Date de la dernière version	10 juin 2005
Source(s)	Bulletins de sécurité 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 ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Squid versions 2.5 et antérieures.

3 Résumé

Plusieurs vulnérabilités sont présentes dans le serveur mandataire Squid permettant à un individu mal intentionné d'effectuer un déni de servcie ou de porter atteinte à l'intégrité des données du serveur mandataire.

4 Description

Squid est un serveur mandataire (`proxy`) pour les protocoles HTTP, HTTPS et FTP.
Le protocole WCCP (`Web Cache Communication Protocol`) est un protocole permettant d'utiliser le serveur mandataire en tant que cache transparent.

Plusieurs vulnérabilités ont été découvertes dans Squid :

- Une vulnérabilité présente dans la fonction `recvfrom()` utilisée pour la réception des requêtes WCCP permet à un individu mal intentionné de réaliser un déni de service sur le serveur affecté par la vulnérabilité via l'envoi d'un paquet WCCP anormalement grand (vulnérabilité CAN-2005-0211) ;
- une vulnérabilité dans le traitement des messages WCCP permet à un individu mal intentionné d'effectuer un déni de service via un message WCCP judicieusement formé (vulnérabilité CVE CAN-2005-0095) ;
- une vulnérabilité présente dans le traitement des requêtes HTTP permet à un individu mal intentionné de polluer le cache du serveur mandataire (vulnérabilités CVE CAN-2005-0173 et CAN-2005-0174) ;
- une vulnérabilité dans la gestion des identifiants LDAP permet à un individu mal intentionné de porter atteinte à l'intégrité des journaux (vulnérabilité CVE CAN-2005-0175) ;
- deux vulnérabilités dans la gestion des authentifications de type NTLM (NT Lan Manager) permet à un individu mal intentionné d'effectuer un déni de service sur le serveur affecté (vulnérabilités CVE CAN-2005-0096 et CAN-2005-0097) ;
- une mauvaise gestion lors de la réception d'entêtes HTTP anormalement grands permettrait à un individu mal intentionné de polluer le cache à distance ou de contourner certaines règles de contrôle d'accès (vulnérabilité CAN-2005-0241).

5 Solution

Se référer aux bulletins de sécurité des éditeurs (cf. section Documentation) pour l'obtention des correctifs.

6 Documentation

- Bulletin de sécurité SQUID-2005:2 du 15 janvier 2005 :
  http://www.squid-cache.org/Advisories/SQUID-2005_02.txt
- Bulletin de sécurité SQUID-2005:3 du 28 janvier 2005 :
  http://www.squid-cache.org/Advisories/SQUID-2005_03.txt
- Bulletin de sécurité Squid du 31 janvier 2005 :
  http://www.squid-cache.org/bugs/show_bug.cgi?id=1200
- Bulletin de sécurité Gentoo GLSA-200501-25 du 16 janvier 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200501-25.xml
- Bulletin de sécurité Gentoo GLSA-200502-04 du 02 février 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200502-04.xml
- Bulletin de sécurité Debian DSA-651 du 20 janvier 2005 :
  http://www.debian.org/security/2005/dsa-651
- Bulletin de sécurité Debian DSA-667 du 04 février 2005 :
  http://www.debian.org/security/2005/dsa-667
- Bulletin de sécurité Mandrake MDKSA-2005:014 du 24 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:014
- Bulletin de sécurité Mandrake MDKSA-2005:034 du 10 février 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:034
- Bulletin de sécurité RedHat (v.2.1 et v.3) RHSA-2005:061 du 11 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-61.html
- Bulletin de sécurité RedHat (v.4) RHSA-2005:060 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-60.html
- Bulletin de sécurité SUSE SuSE-SA:2005:006 du 10 février 2005 :
  http://www.novell.com/linux/security/advisories/2005_06_squid.html
- Bulletin de sécurité OpenBSD pour Squid du 26 janvier 2005 :
  http://www.vuxml.org/openbsd/
- Bulletin de sécurité FreeBSD pour Squid du 28 janvier 2005 :
  http://www.vuxml.org/freebsd/pkg-squid.html
- Bulletin de sécurité FreeBSD pour Squid du 08 février 2005 :
  http://www.vuxml.org/freebsd/pkg-squid.html

- Bulletin de sécurité FreeBSD pour Squid du 03 juin 2005 :
  http://www.vuxml.org/freebsd/pkg-squid.html
- Mise à jour de sécurité du paquetage NetBSD squid :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/squid/README.html
- Référence CVE CAN-2005-0095 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0095
- Référence CVE CAN-2005-0096 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0096
- Référence CVE CAN-2005-0097 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0097
- Référence CVE CAN-2005-0173 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0173
- Référence CVE CAN-2005-0174 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0174
- Référence CVE CAN-2005-0175 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0175
- Référence CVE CAN-2005-0211 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0211
- Référence CVE CAN-2005-0241 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0241
- Note de vulnérabilité #823350 de l'US-CERT :
  http://www.kb.cert.org/vuls/id/823350
- Note de vulnérabilité #886006 de l'US-CERT :
  http://www.kb.cert.org/vuls/id/886006

Gestion détaillée du document

01 février 2005 version initiale.

03 février 2005 mise à jour des vulnérabilités, ajout des références aux bulletins de sécurité OpenBSD, NetBSD, Gentoo et des références CVE CAN-2005-0096, 0097, 0173, 0174, 0175.

11 février 2005 ajout de la référence au bulletin de sécurité Mandrake MDKSA-2005:034.

15 février 2005 ajout des références CVE CAN-2005-0211 et CAN-2005-0241 (nouvelle vulnérabilité), des notes de vulnérabilité de l'US-CERT afférantes, des bulletins de sécurité RedHat et SUSE et de seconds bulletins pour Debian et FreeBSD.

17 février 2005 ajout d'un second bulletin de sécurité RedHat.

10 juin 2005 ajout d'un bulletin de sécurité FreeBSD et modification des références FreeBSD.