Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2004
N° CERTA-2004-AVI-186-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Squid

Gestion du document

Référence	CERTA-2004-AVI-186-003
Titre	Vulnérabilité de Squid
Date de la première version	09 juin 2004
Date de la dernière version	17 juin 2004
Source(s)	Avis de sécurité iDEFENSE du 08 juin 2004
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 à distance.

2 Systèmes affectés

- Toutes les versions de Squid de la branche stable 2.5 ;
- toutes les versions de Squid de la branche de développement 3.0.

Ces versions sont vulnérables sous la condition que le support pour NTLM soit activé lors de la compilation.

3 Résumé

Une vulnérabilité dans le support du protocole d'authentification NTLM permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Squid est un serveur mandataire (proxy) pour les protocoles HTTP, HTTPS et FTP.
Un débordement de mémoire dans le module de gestion du protocole d'authentification NTLM permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance à l'aide d'un mot de passe arbitrairement long.

5 Contournement Provisoire

Recompiler Squid en désactivant le support pour NTLM.

6 Solution

Se référer à la section Documentation pour l'obtention du correctif.
Un correctif pour le code source de Squid est disponible à l'adresse suivante :
http://www.squid-cache.org/~wessels/patch/libntlmssp.c.patch

7 Documentation

- Site Internet de Squid :
  http://www.squid-cache.org
- Avis de sécurité iDEFENSE du 08 juin 2004 :
  http://www.idefense.com/application/poi/display?id=107&type=vulnerabilities
- Bulletin de sécurité MDKSA-2004:059 de Mandrake du 09 juin 2004 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:059
- Bulletin de sécurité SuSE-SA:2004:016 de SuSE du 09 juin 2004 :
  http://www.suse.com/de/security/2004_16_squid.html
- Bulletin de sécurité RHSA-2004-242 de Red Hat du 09 juin 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-242.html
- Avis de sécurité FreeBSD sur Squid du 09 juin 2004 :
  http://www.vuxml.org/freebsd/
- Avis de sécurité Gentoo GLSA 200406-13 du 17 juin 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200406-13.xml
- Référence CVE CAN-2004-0541 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0541

Gestion détaillée du document

09 juin 2004 version initiale.
10 juin 2004 ajout des références aux avis de Mandrake, SuSE et Red Hat.
14 juin 2004 ajout de la référence à l'avis de sécurité FreeBSD.
17 juin 2004 ajout de la référence à l'avis de sécurité Gentoo.