

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-2004-AVI-297>

Gestion du document

Référence	CERTA-2004-AVI-297-001
Titre	Vulnérabilité de Squid
Date de la première version	03 septembre 2004
Date de la dernière version	16 septembre 2004
Source(s)	Bulletin de sécurité Gentoo GLSA 200409-04 du 02 septembre 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

Déni de service.

2 Systèmes affectés

Toutes les versions de Squid de la branche stable 2.5.
Ces versions sont vulnérables sous la condition que la prise en compte du protocole NTLM soit activée lors de la compilation.

3 Résumé

Une vulnérabilité dans la gestion du protocole d'authentification NTLM permet à un utilisateur mal intentionné de réaliser un déni de service.

4 Description

Squid est un serveur mandataire (proxy) pour les protocoles HTTP, HTTPS et FTP.
Deux failles dans des fonctions relatives à la gestion du protocole d'authentification NTLM (`ntlm_fetch_string()`)

et `ntlm_get_string()` permettent à un utilisateur mal intentionné de réaliser un déni de service sur la plateforme vulnérable.

5 Contournement Provisoire

Recompiler Squid en désactivant la prise en charge du protocole 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://www1.uk.squid-cache.org/squid/Versions/v2/2.5/bugs/squid-2.5.STABLE6-ntlm_fetch_string.patch

7 Documentation

- Site Internet de Squid :
<http://www.squid-cache.org>
- Bulletin de sécurité Squid du 20 août 2004 :
http://www1.uk.squid-cache.org/squid/Versions/v2/2.5/bugs/#squid-2.5.STABLE6-ntlm_fetch_string
- Bulletin de sécurité Gentoo GLSA 200409-04 du 02 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-04.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:093 du 15 septembre 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:093>
- Référence CVE CAN-2004-0832 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0832>

Gestion détaillée du document

03 septembre 2004 version initiale.

16 septembre 2004 ajout référence au bulletin de sécurité de Mandrake. Ajout référence CVE.