

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-348>

Gestion du document

Référence	CERTA-2004-AVI-348-004
Titre	Vulnérabilité de Squid
Date de la première version	20 octobre 2004
Date de la dernière version	22 novembre 2004
Source(s)	Bulletin de sécurité d'iDEFENSE du 11 octobre 2004 Bulletin de sécurité GLSA 200410-15 de Gentoo
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 2.5.Stable6 et versions antérieures.

3 Description

Squid est un serveur mandataire (proxy) pour les protocoles HTTP, HTTPS et FTP.

Une vulnérabilité est présente dans la routine `asn_parse_header()` appelée lors du traitement des paquets SNMP. Via le biais de requêtes SNMP habilement constituées, un utilisateur mal intentionné peut forcer l'arrêt brutal du serveur Squid.

4 Contournement provisoire

Désactiver le support SNMP au niveau du serveur Squid ou filtrer les accès au port utilisé par le module SNMP du serveur Squid (3401/UDP par défaut).

5 Solution

La version 2.5.Stable7 corrige cette vulnérabilité.

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

6 Documentation

- Sources de Squid :
<http://www.squid-cache.org>
- Nouveautés de la version 2.5.Stable7 sur le site de Squid :
<http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE7-RELEASENOTES.html>
- Bulletin de sécurité d'iDEFENSE du 11 octobre 2004 :
<http://www.odefense.com/application/poi/display?id=152&type=vulnerabilities>
- Bulletin de sécurité Gentoo GLSA 200410-15 de Gentoo :
<http://www.gentoo.org/security/en/glsa/glsa-200410-15.xml>
- Bulletin de sécurité Red Hat RHSA-2004:591 du 20 octobre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-591.html>
- Bulletin de sécurité Mandrake MDKSA-2004:112 du 22 octobre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:112>
- Bulletin de sécurité Debian DSA-576 du 29 octobre 2004 :
<http://www.debian.org/security/2004/dsa-576>
- Bulletin de sécurité OpenBSD pour squid du 20 octobre 2004 :
<http://www.vuxml.org/openbsd/>
- Référence CVE CAN-2004-0918 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0918>

Gestion détaillée du document

20 octobre 2004 version initiale.

21 octobre 2004 ajout de la référence au bulletin de sécurité de Red Hat.

22 octobre 2004 ajout de la référence au bulletin de sécurité de Mandrake.

29 octobre 2004 ajout de la référence au bulletin de sécurité de Debian.

22 novembre 2004 ajout de la référence au bulletin de sécurité de OpenBSD.