



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mai 2004
N° CERTA-2004-AVI-062-006

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-062>

Gestion du document

Référence	CERTA-2004-AVI-062-006
Titre	Vulnérabilité de Squid
Date de la première version	03 mars 2004
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité de Squid SQUID-2004:1
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

Contournement de la politique de sécurité.

2 Systèmes affectés

Squid versions 2.5.STABLE4 et antérieures.

3 Résumé

Deux vulnérabilités dans Squid permettent à un utilisateur mal intentionné de contourner la politique de sécurité mise en place.

4 Description

Squid est un serveur mandataire (proxy) pour les protocoles HTTP, HTTPS et FTP. Deux vulnérabilités ont été identifiées dans Squid permettant à un utilisateur mal intentionné de contourner la politique de sécurité, notamment de contourner les contrôles d'accès basés sur la directive `url_regex`.

5 Solution

Mettre à jour Squid en version 2.5.STABLE5 ou appliquer le correctif fournit par l'éditeur :

- Site pour le téléchargement de Squid :
<http://www.squid-cache.org/Versions/v2/2.5/>
- Bulletin de sécurité RHSA-2004:133 pour Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-133.html>
- Bulletin de sécurité RHSA-2004:134 pour Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-134.html>
- Bulletin de sécurité MDKSA-2004:025 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:025>
- Bulletin de sécurité GLSA 200403-11 de Gentoo :
<http://www.securityfocus.com/advisories/6495>
- Bulletin de sécurité DSA-474 de Debian :
<http://www.debian.org/security/2004/dsa-474>
- Bulletin de sécurité SGI 20040404-01-U du 21 avril 2004 :
<ftp://patches.sgi.com/support/free/security/advisories/20040404-01-U.asc>

Note : pour vérifier la version de Squid, taper la commande :
`squid -v`

6 Documentation

- Avis de sécurité de Squid SQUID-2004:1 du 29 février 2004 :
http://www.squid-cache.org/Advisories/SQUID-2004_1.txt
- Avis de sécurité FreeBSD du 26 mars mars 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD squid :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Référence CVE CAN-2004-0189 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0189>

Gestion détaillée du document

03 mars 2004 version initiale.

30 mars 2004 ajout référence au bulletin de sécurité de Red Hat. Ajout référence CVE.

31 mars 2004 ajout référence au bulletin de sécurité de Mandrake.

01 avril 2004 ajout référence au bulletin de sécurité de Gentoo.

05 avril 2004 ajout référence au bulletin de sécurité de Debian.

10 mai 2004 ajout des références aux bulletins de sécurité RedHat et SGI.

12 mai 2004 ajout des références aux bulletins de sécurité FreeBSD et NetBSD.