



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 novembre 2009
N° CERTA-2009-AVI-468

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans SquidGuard

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-2009-AVI-468>

Gestion du document

Référence	CERTA-2009-AVI-468
Titre	Multiples vulnérabilités dans SquidGuard
Date de la première version	03 novembre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité SquidGuard du 15 et 19 octobre 2009
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

- SquidGuard 1.3 ;
- SquidGuard 1.4.

3 Résumé

Plusieurs vulnérabilités présentes dans SquidGuard permettent à un utilisateur distant malintentionné de contourner la politique de sécurité.

4 Description

Deux vulnérabilités sont présentes dans SquidGuard :

- la première concerne une fonction du fichier *sgLog.c* qui, sous certaines conditions, fait passer SquidGuard en mode d'urgence ; ce qui a pour effet de désactiver le filtrage ;

- la seconde vulnérabilité est liée à un problème dans le traitement des URLs de très grande taille qui empêche un filtrage correct des liens analysés.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletins de sécurité de SquidGuard du 15 et du 19 octobre 2009 :
<http://www.squidguard.org/Downloads/Patches/1.3/Readme.Patch-20091015>
<http://www.squidguard.org/Downloads/Patches/1.3/Readme.Patch-20091019>
<http://www.squidguard.org/Downloads/Patches/1.4/Readme.Patch-20091015>
<http://www.squidguard.org/Downloads/Patches/1.4/Readme.Patch-20091019>
- Référence CVE CVE-2009-3700 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3700>
- Référence CVE CVE-2009-3826 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3826>

Gestion détaillée du document

03 novembre 2009 version initiale.