

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Google Chrome

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-500>

Gestion du document

Référence	CERTA-2009-AVI-500
Titre	Vulnérabilité dans Google Chrome
Date de la première version	13 novembre 2009
Date de la dernière version	–
Source(s)	Bulletin de mise à jour Google du 12 novembre 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 ;
- injection de requêtes illégitimes par rebond.

2 Systèmes affectés

Google Chrome 3.x.

3 Résumé

Une vulnérabilité dans *Google Chrome* permet à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

La gestion des en-têtes HTTP envoyés par *Google Chrome* lors de l'accès à des ressources partagées entre domaines permet de contourner la politique de sécurité. En particulier, elle facilite les injections de requêtes illégitimes par rebond (CSRF).

5 Solution

Mettre à jour en version 3.0.195.33.

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

6 Documentation

- Bulletin de mise à jour Google du 12 novembre 2009 :
<http://googlechromereleases.blogspot.com/2009/11/stable-update-fix-google-chrome-not.html>
- Référence CVE CVE-2009-2816 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2816>

Gestion détaillée du document

13 novembre 2009 version initiale.