

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mutiples vulnérabilités du navigateur 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-401>

Gestion du document

Référence	CERTA-2009-AVI-401
Titre	Mutiples vulnérabilités du navigateur Google Chrome
Date de la première version	24 septembre 2009
Date de la dernière version	–
Source(s)	Bloc-notes Google Chrome
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 code indirecte.

2 Systèmes affectés

Google Chrome versions antérieures à la version 3.0.195.21.

3 Résumé

Des vulnérabilités permettant de réaliser de l'injection de code indirecte ont été découvertes dans le navigateur *Google Chrome*.

4 Description

Deux vulnérabilités ont été découvertes dans le navigateur *Google Chrome* :

- la première résulte d'une mauvaise gestion des flux RSS et Atom et permet d'exécuter du code indirect via un flux spécialement construit ;

- la seconde est due à une erreur au niveau de la méthode `getSVGDocument` et permet d'exécuter du code HTML ou du script à distance via un document SVG spécialement construit.

5 Solution

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

6 Documentation

- Bloc-notes Google Chrome :
<http://googlechromereleases.blogspot.com/2009/09/stable-channel-update.html>
- Référence CVE CVE-2009-3263 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3263>
- Référence CVE CVE-2009-3264 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3264>

Gestion détaillée du document

24 septembre 2009 version initiale.