Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 juillet 2010
N° CERTA-2010-AVI-300

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Google Chrome

Gestion du document

Référence	CERTA-2010-AVI-300
Titre	Multiples vulnérabilités dans Google Chrome
Date de la première version	05 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Google Chrome du 2 juillet 2010
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

`Google Chrome` versions antérieures à 5.0.375.99 pour GNU/Linux, Mac OS X et Microsoft Windows.

3 Résumé

De multiples vulnérabilités présentes dans `Google Chrome` permettent à un utilisateur malintentionné distant de contourner la politique de sécurité, ou d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités sont présentes dans le navigateur Web `Google Chrome`. Celles-ci permettent à un utilisateur distant malintentionné de contourner certains mécanismes de protection mis en oeuvre dans `Chrome`, par le biais de pages Web construites de façon particulière. Citons :

– une vulnérabilité dans `WebGL` ;

- une vulnérabilité dans le mécanisme d'isolation "bac à sable" des `iframes` ;
- une vulnérabilité dans la gestion des images `SVG` et `PNG` ;
- une vulnérabilité dans l'algorithme `bidi` ;
- une vulnérabilité dans la gestion d'images invalides ;
- une vulnérabilité dans la gestion des styles `CSS` ;
- une vulnérabilité dans les boites messages et les fenêtres d'impressions.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La version 5.0.375.99 de `Google Chrome` corrige ces vulnérabilités.

6 Documentation

- Bulletin de sécurité de `Google Chrome` du 2 juillet 2010 :
  http://googlechromereleases.blogspot.com/2010/07/stable-channel-update.html

Gestion détaillée du document

05 juillet 2010 version initiale.