

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-2012-AVI-197>

---

### Gestion du document

Référence	CERTA-2012-AVI-197
Titre	Multiples vulnérabilités dans Google Chrome
Date de la première version	10 avril 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Google Chrome du 05 avril 2012
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Versions antérieures à Google Chrome 18.0.1025.151.

## 3 Résumé

Douze vulnérabilités ont été corrigées dans *Google Chrome*. Trois types de vulnérabilités sont présents. Le premier est une utilisation de données après la libération de l'espace mémoire (*use after free*), il concerne huit des vulnérabilités. Le deuxième permet de lire des données dans une zone non autorisée, il concerne deux des vulnérabilités. Le dernier contourne les cloisonnements d'informations appelés « *Cross-origin* », deux vulnérabilités sont concernées.

## 4 Solution

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

## 5 Documentation

- Note de version Google Chrome 2012/04/stable-and-beta-channel-updates du 05 avril 2012 :  
<http://googlechromereleases.blogspot.com/2012/04/stable-and-beta-channel-updates.html>
- Référence CVE CVE-2011-3066 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3066>
- Référence CVE CVE-2011-3067 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3067>
- Référence CVE CVE-2011-3068 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3068>
- Référence CVE CVE-2011-3069 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3069>
- Référence CVE CVE-2011-3070 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3070>
- Référence CVE CVE-2011-3071 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3071>
- Référence CVE CVE-2011-3072 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3072>
- Référence CVE CVE-2011-3073 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3073>
- Référence CVE CVE-2011-3074 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3074>
- Référence CVE CVE-2011-3075 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3075>
- Référence CVE CVE-2011-3076 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3076>
- Référence CVE CVE-2011-3077 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3077>

### Gestion détaillée du document

**10 avril 2012** version initiale.