

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-030>

Gestion du document

Référence	CERTA-2012-AVI-030
Titre	Multiples vulnérabilités dans Google Chrome
Date de la première version	25 janvier 2012
Date de la dernière version	–
Source(s)	Note de version Google Chrome stable channel update du 23 janvier 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 ;
- déni de service à distance.

2 Systèmes affectés

Google Chrome versions antérieures à 16.0.912.77.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans Google Chrome, qui peuvent être exploitées pour exécuter du code arbitraire à distance ou réaliser un déni de service à distance.

4 Description

Cinq vulnérabilités ont été corrigées dans Google Chrome. Trois concernent l'utilisation d'un pointeur après libération, (CVE-2011-3924, 3925, 3928), une l'utilisation d'une variable sans initialisation (CVE-2011-3927), et la dernière un dépassement de tampon dans la pile (CVE-2011-3926).

5 Solution

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

6 Documentation

- Note de version Google Chrome stable channel update du 23 janvier 2012 :
http://googlechromereleases.blogspot.com/2012/01/stable-channel-update_23.html
- Référence CVE CVE-2011-3924 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3924>
- Référence CVE CVE-2011-3925 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3925>
- Référence CVE CVE-2011-3926 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3926>
- Référence CVE CVE-2011-3927 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3927>
- Référence CVE CVE-2011-3928 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3928>

Gestion détaillée du document

25 janvier 2012 version initiale.