Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mai 2009
N° CERTA-2009-AVI-180

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Google Chrome

Gestion du document

Référence	CERTA-2009-AVI-180
Titre	Vulnérabilités dans Google Chrome
Date de la première version	11 mai 2009
Date de la dernière version	–
Source(s)	Rapport de bogue #10869 de Google Chromium du 22 avril 2009 Rapport de bogue #10736 de Google Chromium du 19 avril 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Google Chrome versions antérieures à 1.0.154.64.

3 Résumé

Deux vulnérabilités dans *Google Chrome* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été corrigées dans *Google Chrome* :

– un débordement de mémoire dans la fonction `ParamTraits<SkBitmap>::Read` permet à une personne malintentionnée d'effectuer un déni de service voire d'exécuter du code arbitraire (CVE-2009-1441) ;

– un débordement d'entier dans le calcul de taille d'images permet à une personne malintentionnée distante d'effectuer un déni de service voire d'exécuter du code arbitraire au moyen d'une image spécialement conçue (CVE-2009-1442).

5 Solution

Les deux vulnérabilités sont corrigées dans la version 1.0.154.64.

6 Documentation

– Rapport de bogue #10736 de Google Chromium du 19 avril 2009 :
http://code.google.com/p/chromium/issues/details?id=10736
– Rapport de bogue #10869 de Google Chromium du 22 avril 2009 :
http://code.google.com/p/chromium/issues/details?id=10869
– Bloc-notes de suivi de versions de Google Chrome :
http://googlechromreleases.blogspot.com
– Référence CVE CVE-2009-1441 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1441
– Référence CVE CVE-2009-1442 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1442

Gestion détaillée du document

11 mai 2009 version initiale.