

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-355>

Gestion du document

Référence	CERTA-2009-AVI-355
Titre	Multiples vulnérabilités du navigateur Google Chrome
Date de la première version	27 août 2009
Date de la dernière version	–
Source(s)	Note de mise à jour Google Chrome du 25 août 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Google Chrome versions antérieures à la version 2.0.172.43.

3 Résumé

Plusieurs vulnérabilités permettant, entre autres, l'exécution de code arbitraire à distance ont été découvertes dans Google Chrome.

4 Description

Plusieurs vulnérabilités ont été découvertes dans le navigateur Google Chrome :

- la première vulnérabilité est due à une erreur dans le moteur d'interprétation du langage javascript et permet à un utilisateur malveillant d'accéder à la mémoire ;
- la deuxième vulnérabilité est due à une mauvaise gestion des certificats SSL, permettant ainsi de contourner les mécanismes de confidentialité mis en place ;
- les deux dernières vulnérabilités sont issues de l'utilisation d'une version vulnérable de la bibliothèque libxml2, et permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Note de mise à jour Google Chrome du 25 août 2009 :
<http://googlechromereleases.blogspot.com/2009/08/stable-update-security-fixes.html>
- Référence CVE CVE-2009-2935 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2935>
- Référence CVE CVE-2009-2414 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2414>
- Référence CVE CVE-2009-2416 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2416>

Gestion détaillée du document

27 août 2009 version initiale.