Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 mars 2010
N° CERTA-2010-AVI-132

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Qt

Gestion du document

Référence	CERTA-2010-AVI-132
Titre	Multiples vulnérabilités dans Qt
Date de la première version	24 mars 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurité Fedora FEDORA-2010-4518, 4521 et 4524 du 15 mars 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Qt 4.x.

3 Résumé

Plusieurs vulnérabilités affectent Qt et permettent l'exécution de code arbitraire à distance ou l'accès à des informations sensibles par un utilisateur malintentionné.

4 Description

Une vulnérabilité (CVE-2010-0051) dans la gestion des feuilles de style (CSS) par Qt est exploitable par un utilisateur malintentionné pour obtenir des informations sensibles au moyen d'une page HTML spécialement conçue.

Plusieurs vulnérabilités permettent à un utilisateur malveillant de provoquer un arrêt inopiné ou d'exécuter du code arbitraire à distance. Ces vulnérabilités utilisent des éléments de type IMG ou de type INPUT, des fonctions ou des défauts d'imbrication dans des pages HTML, ou encore des formats dans des feuilles de styles CSS.

5 Solution

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

6 Documentation

- Bulletin de sécurité Fedora FEDORA-2010-4518
  https://admin.fedoraproject.org/updates/qt-4.6.2-8.fc12
- Bulletin de sécurité Fedora FEDORA-2010-4521
  https://admin.fedoraproject.org/updates/qt-4.6.2-8.fc13
- Bulletin de sécurité Fedora FEDORA-2010-4524
  https://admin.fedoraproject.org/updates/qt-4.6.2-8.fc11
- Référence CVE CVE-2010-0046 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0046
- Référence CVE CVE-2010-0049 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0049
- Référence CVE CVE-2010-0050 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0050
- Référence CVE CVE-2010-0051 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0051
- Référence CVE CVE-2010-0052 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0052
- Référence CVE CVE-2010-0054 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0054

Gestion détaillée du document

24 mars 2010 version initiale.