Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 octobre 2009
N° CERTA-2009-AVI-460

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Opera

Gestion du document

Référence	CERTA-2009-AVI-460
Titre	Vulnérabilités dans Opera
Date de la première version	28 octobre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Opera
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Opera versions antérieures à 10.01.

3 Résumé

Des vulnérabilités dans *Opera* permettent notamment une exécution de code arbitraire à distance.

4 Description

Trois vulnérabilités ont été découvertes dans *Opera* :

- certains noms de domaine spécifiques peuvent provoquer une corruption de la mémoire. Cette vulnérabilité peut être exploitée pour exécuter du code arbitraire à distance ;

- les scripts sont autorisés à être exécutés sur la page d'inscription aux flux ce qui peut être utilisé pour s'abonner automatiquement ou lire des flux non prévus ;
- dans certains cas, une police Web prévue pour le contenu d'une page peut être utilisée pour l'affichage de l'interface utilisateur. Un site malintentionné peut exploiter cette vulnérabilité pour afficher un faux nom de domaine dans la barre de navigation.

5 Solution

Mettre *Opera* à jour en version 10.01.

6 Documentation

- Bulletins de sécurité Opera :
  http://www.opera.com/support/kb/view/938/
  http://www.opera.com/support/kb/view/939/
  http://www.opera.com/support/kb/view/940/
- Page de téléchargement d'Opera :
  http://www.opera.com/browser/

Gestion détaillée du document

28 octobre 2009 version initiale.