Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juin 2012
N° CERTA-2012-AVI-338

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Opera

Gestion du document

Référence	CERTA-2012-AVI-338
Titre	Multiples vulnérabilités dans Opera
Date de la première version	19 juin 2012
Date de la dernière version	–
Source(s)	Bulletins de sécurité Opera 1018 à 1022
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 ;
- injection de code indirecte à distance.

2 Systèmes affectés

Versions antérieures à Opera 11.65.

3 Résumé

Cinq vulnérabilités ont été corrigées dans *Opera*. Deux peuvent mener à une falsification de l'URL, une permet d'accéder à des données JSON sensibles. Les deux dernières requièrent une interaction avec l'utilisateur et peuvent mener à une injection de code indirecte à distance (XSS) ou à une exécution de code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Opera 1018 :
  http://www.opera.com/support/kb/view/1018/
- Bulletin de sécurité Opera 1019 :
  http://www.opera.com/support/kb/view/1019/
- Bulletin de sécurité Opera 1020 :
  http://www.opera.com/support/kb/view/1020/
- Bulletin de sécurité Opera 1021 :
  http://www.opera.com/support/kb/view/1021/
- Bulletin de sécurité Opera 1022 :
  http://www.opera.com/support/kb/view/1022/

Gestion détaillée du document

19 juin 2012 version initiale.