Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juin 2012
N° CERTA-2012-AVI-351

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans IBM Lotus Expeditor

Gestion du document

Référence	CERTA-2012-AVI-351
Titre	Multiples vulnérabilités dans IBM Lotus Expeditor
Date de la première version	25 juin 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM swg21575642 du 21 juin 2012
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 ;
- injection de code indirecte à distance.

2 Systèmes affectés

Versions antérieures à IBM Lotus Expeditor 6.2 FP5+Security Pack.

3 Résumé

Cinq vulnérabilités ont été corrigées dans *IBM Lotus Expeditor*. Elles sont réparties comme suit :
- (CVE-2012-0186) une URL spécialement conçue permet de lire arbitrairement des ressources sensibles ;
- (CVE-2012-0191) en modifiant son en-tête HTTP un attaquant peut contourner les restrictions du serveur à certaines zones ;
- (CVE-2012-0187) le chargement d'une bibliothèque (DLL) arbitraire lors du chargement de certains fichiers ;
- (CVE-2008-7271 et CVE-2008-4647) deux injections de code indirecte à distance (XSS).

4 Solution

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

5 Documentation

- Bulletin de sécurité IBM swg21575642 du 21 juin 2012 :
  http://www-01.ibm.com/support/docview.wss?uid=swg21575642
- Référence CVE CVE-2012-0191 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0191
- Référence CVE CVE-2012-0187 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0187
- Référence CVE CVE-2012-0186 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0186
- Référence CVE CVE-2008-7271 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-7271
- Référence CVE CVE-2008-4647 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4647

Gestion détaillée du document

25 juin 2012 version initiale.