Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 20 août 2014
N° CERTFR-2014-AVI-364

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits IBM

Gestion du document

Référence	CERTFR-2014-AVI-364
Titre	Multiples vulnérabilités dans les produits IBM
Date de la première version	20 août 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM SWG21681651 du 20 août 2014 Bulletin de sécurité IBM SWG21680403 du 20 août 2014 Bulletin de sécurité IBM SWG21681649 du 20 août 2014 Bulletin de sécurité IBM SWG21680603 du 20 août 2014 Bulletin de sécurité IBM SWG21681528 du 20 août 2014 Bulletin de sécurité IBM SWG21677691 du 20 août 2014 Bulletin de sécurité IBM SWG21679726 du 20 août 2014
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(s)

- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- IBM InfoSphere Master Data Management versions 10.1 et 10.0
- IBM InfoSphere Master Data Management Server versions 9.1 et 9.0
- IBM Rational Build Forge versions 7.1.2.0 à 7.1.2.3
- IBM UrbanCode Release versions 6.0 à 6.1
- IBM Enterprise Records versions 4.5 à 5.1.2
- IBM Business Process Manager versions 8.0 à 8.5.5
- IBM WebSphere Lombardi Edition version 7.2

3 - Résumé

De multiples vulnérabilités ont été corrigées dans des produits *IBM*. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.

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 SWG21681649 du 20 août 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21681649
- Bulletin de sécurité IBM SWG21681651 du 20 août 2014
  https://www.ibm.com/support/docview.wss?uid=swg21681651
- Bulletin de sécurité IBM SWG21680403 du 20 août 2014
  https://www.ibm.com/support/docview.wss?uid=swg21680403
- Bulletin de sécurité IBM SWG21680603 du 20 août 2014
  https://www.ibm.com/support/docview.wss?uid=swg21680603
- Bulletin de sécurité IBM SWG21681528 du 20 août 2014
  http://www.ibm.com/support/docview.wss?uid=swg21681528
- Bulletin de sécurité IBM SWG21677691 du 20 août 2014
  http://www.ibm.com/support/docview.wss?uid=swg21677691
- Bulletin de sécurité IBM SWG21679726 du 20 août 2014
  http://www.ibm.com/support/docview.wss?uid=swg21679726
- Référence CVE CVE-2014-3087
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3087
- Référence CVE CVE-2014-0050
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0050
- Référence CVE CVE-2014-0966
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0966
- Référence CVE CVE-2014-0969
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0969
- Référence CVE CVE-2014-3063
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3063

Gestion détaillée du document

20 août 2014 version initiale.