

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits IBM

Gestion du document

Référence	CERTFR-2014-AVI-525
Titre	Multiples vulnérabilités dans les produits IBM
Date de la première version	11 décembre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM du 10 décembre 2014 Bulletin de sécurité IBM du 10 décembre 2014 Bulletin de sécurité IBM du 10 décembre 2014 Bulletin de sécurité IBM du 10 décembre 2014 Bulletin de sécurité IBM du 10 décembre 2014 Bulletin de sécurité IBM du 10 décembre 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 la confidentialité des données
- injection de code indirecte à distance

2 - Systèmes affectés

- IBM WebSphere Portal 8.x
- IBM Rational ClearQuest 7.x
- IBM Rational ClearQuest 8.x
- IBM Rational RequisitePro 7.x
- IBM Integration Bus 9.x
- IBM WebSphere Message Broker 7.x
- IBM WebSphere Message Broker 8.x
- IBM Rational ClearCase 7.x
- IBM Rational ClearCase 8.x

- IBM Cognos Business Intelligence 10.x

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les 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 la confidentialité des données.

4 - Contournement provisoire

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

5 - Documentation

- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg21691458>
- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg21692062>
- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg24038916>
- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg21692139>
- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg21692062>
- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg24038912>
- Bulletin de sécurité IBM du 10 décembre 2014
<http://www.ibm.com/support/docview.wss?uid=swg24038915>
- Référence CVE CVE-2014-6215
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6215>
- Référence CVE CVE-2014-3509
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3509>
- Référence CVE CVE-2014-3511
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3511>
- Référence CVE CVE-2014-5139
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5139>
- Référence CVE CVE-2014-4244
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4244>
- Référence CVE CVE-2014-4263
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4263>
- Référence CVE CVE-2014-4815
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4815>
- Référence CVE CVE-2014-3065
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3065>
- Référence CVE CVE-2014-4288
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4288>
- Référence CVE CVE-2014-6457
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6457>
- Référence CVE CVE-2014-6458
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6458>
- Référence CVE CVE-2014-6466
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6466>
- Référence CVE CVE-2014-6468
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6468>

- Référence CVE CVE-2014-6476
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6476>
- Référence CVE CVE-2014-6492
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6492>
- Référence CVE CVE-2014-6493
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6493>
- Référence CVE CVE-2014-6502
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6502>
- Référence CVE CVE-2014-6503
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6503>
- Référence CVE CVE-2014-6504
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6504>
- Référence CVE CVE-2014-6506
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6506>
- Référence CVE CVE-2014-6511
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6511>
- Référence CVE CVE-2014-6512
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6512>
- Référence CVE CVE-2014-6513
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6513>
- Référence CVE CVE-2014-6515
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6515>
- Référence CVE CVE-2014-6517
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6517>
- Référence CVE CVE-2014-6519
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6519>
- Référence CVE CVE-2014-6527
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6527>
- Référence CVE CVE-2014-6531
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6531>
- Référence CVE CVE-2014-6532
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6532>
- Référence CVE CVE-2014-6546
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6546>
- Référence CVE CVE-2014-6558
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6558>
- Référence CVE CVE-2014-6562
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6562>

Gestion détaillée du document

11 décembre 2014 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-525>
