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 22 avril 2014
N° CERTFR-2014-AVI-199

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits IBM

Gestion du document

Référence	CERTFR-2014-AVI-199
Titre	Multiples vulnérabilités dans les produits IBM
Date de la première version	22 avril 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM N1020021 du 18 avril 2014 Bulletin de sécurité IBM 1670738 du 18 avril 2014 Bulletin de sécurité IBM S1004599 du 16 avril 2014 Bulletin de sécurité IBM N1020038 du 18 avril 2014 Bulletin de sécurité IBM 1670864 du 18 avril 2014 Bulletin de sécurité IBM 1670858 du 22 avril 2014 Bulletin de sécurité IBM 1668578 du 18 avril 2014 Bulletin de sécurité IBM 1670750 du 17 avril 2014 Bulletin de sécurité IBM 1669459 du 18 avril 2014 Bulletin de sécurité IBM T1020715 du 18 avril 2014 Bulletin de sécurité IBM 1664531 du 18 avril 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)

- non spécifié par l'éditeur
- exécution de code arbitraire à distance
- déni de service
- atteinte à la confidentialité des données

2 - Systèmes affectés

- IBM HMC V7 Release 7.7.0
- IBM HMC V7 Release 7.8.0
- IBM Initiate Master Data Service version 9.5
- IBM Initiate Master Data Service version 9.7

- IBM Initiate Master Data Service version 10.0
- IBM Initiate Master Data Service version 10.1
- IBM Initiate Master Data Service Patient Hub version 9.5
- IBM Initiate Master Data Service Patient Hub version 9.7
- IBM Initiate Master Data Service Provider Hub version 9.5
- IBM Initiate Master Data Service Provider Hub version 9.7
- IBM InfoSphere Master Data Management Patient Hub version 10.0
- IBM InfoSphere Master Data Management Provider Hub version 10.0
- IBM InfoSphere Master Data Management Standard/Advanced Edition version 11.0
- IBM TS3000 (TSSC) version 7.2.x
- IBM i version V5R3
- IBM i version V5R4
- IBM i version 6.1
- IBM i version 7.1
- IBM Worklight Consumer Edition version 6.1.0.0
- IBM Worklight Consumer Edition version 6.1.0 Fix Pack 1
- IBM Worklight Enterprise Edition Versions 6.1.0.0
- IBM Worklight Enterprise Edition version 6.1.0 Fix Pack 1
- IBM Tivoli Storage Productivity Center versions 5.2.1.0 et antérieures
- IBM Tivoli Storage Productivity Center versions 5.1.1.3 et antérieures
- IBM Tivoli Storage Productivity Center versions 4.2.2.177 et antérieures
- IBM Tivoli Provisioning Manager for Software 5.1
- IBM SmartCloud Provisioning 2.3.0
- IBM Connections 3.0.1.1 et versions antérieures
- IBM Connections 4.0
- IBM Connections 4.5
- IBM SDN VE, Unified Controller, VMware Edition: 1.0.0
- IBM SDN VE, Unified Controller, KVM Edition: 1.0.0
- IBM SDN VE, Unified Controller, OpenFlow Edition: 1.0.0
- IBM SDN VE, Dove Management Console, VMware Edition: 1.0.0
- IBM Rational Software Architect Design Manager version 4.0.5
- IBM Rational Software Architect Design Manager version 4.0.4
- IBM Rational Software Architect Design Manager version 4.0.3
- IBM Rational Software Architect Design Manager version 4.0.2
- IBM Rational Software Architect Design Manager version 4.0.1
- IBM Rational Software Architect Design Manager version 4.0
- IBM Rational Software Architect Design Manager version 3.0.1
- IBM Rational Software Architect Design Manager version 3.0.0.1
- IBM Rational Software Architect Design Manager version 3.0
- IBM Rhapsody Design Manager version 4.0.5
- IBM Rhapsody Design Manager version 4.0.4
- IBM Rhapsody Design Manager version 4.0.3
- IBM Rhapsody Design Manager version 4.0.2
- IBM Rhapsody Design Manager version 4.0.1
- IBM Rhapsody Design Manager version 4.0
- IBM Rhapsody Design Manager version 3.0.1
- IBM Rhapsody Design Manager version 3.0.0.1
- IBM Rhapsody Design Manager version 3.0

3 - Résumé

De multiples vulnérabilités ont été corrigées dans les produits *IBM*. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et un déni de service.

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 N1020021 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=nas8N1020021
- Bulletin de sécurité IBM 1670738 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21670738
- Bulletin de sécurité IBM S1004599 du 16 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004599
- Bulletin de sécurité N1020038 IBM du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=nas8N1020038
- Bulletin de sécurité IBM 1670864 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21670864
- Bulletin de sécurité IBM 1670858 du 22 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21670858
- Bulletin de sécurité IBM 1668578 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21668578
- Bulletin de sécurité IBM 1670750 du 17 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21670750
- Bulletin de sécurité IBM 1669459 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21669459
- Bulletin de sécurité IBM T1020715 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=isg3T1020715
- Bulletin de sécurité IBM 1664531 du 18 avril 2014
  http://www-01.ibm.com/support/docview.wss?uid=swg21664531
- Référence CVE CVE-2013-5763
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5763
- Référence CVE CVE-2013-5791
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5791
- Référence CVE CVE-2013-5879
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5879
- Référence CVE CVE-2014-0076
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0076
- Référence CVE CVE-2013-4353
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4353
- Référence CVE CVE-2013-6449
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6449
- Référence CVE CVE-2014-0160
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- Référence CVE CVE-2013-3829
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3829
- Référence CVE CVE-2013-4041
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4041
- Référence CVE CVE-2013-5372
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5372
- Référence CVE CVE-2013-5375
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5375
- Référence CVE CVE-2013-5774
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5774
- Référence CVE CVE-2013-5778
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5778

- Référence CVE CVE-2013-5780
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5780
- Référence CVE CVE-2013-5782
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5782
- Référence CVE CVE-2013-5783
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5783
- Référence CVE CVE-2013-5790
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5790
- Référence CVE CVE-2013-5797
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5797
- Référence CVE CVE-2013-5801
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5801
- Référence CVE CVE-2013-5802
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5802
- Référence CVE CVE-2013-5803
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5803
- Référence CVE CVE-2013-5804
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5804
- Référence CVE CVE-2013-5809
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5809
- Référence CVE CVE-2013-5814
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5814
- Référence CVE CVE-2013-5817
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5817
- Référence CVE CVE-2013-5825
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5825
- Référence CVE CVE-2013-5829
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5829
- Référence CVE CVE-2013-5830
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5830
- Référence CVE CVE-2013-5840
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5840
- Référence CVE CVE-2013-5842
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5842
- Référence CVE CVE-2013-5843
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5843
- Référence CVE CVE-2013-5849
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5849
- Référence CVE CVE-2013-5850
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5850
- Référence CVE CVE-2013-5907
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5907
- Référence CVE CVE-2014-0368
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0368
- Référence CVE CVE-2014-0373
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0373
- Référence CVE CVE-2014-0376
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0376
- Référence CVE CVE-2014-0411
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0411
- Référence CVE CVE-2014-0416
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0416
- Référence CVE CVE-2014-0417
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0417

- Référence CVE CVE-2014-0422
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0422
- Référence CVE CVE-2014-0423
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0423
- Référence CVE CVE-2014-0428
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0428
- Référence CVE CVE-2013-5459
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5459

Gestion détaillée du document

22 avril 2014 version initiale.