IBM PSIRT Quarterly Security Bulletin Summary – 4th Quarter 2011

This document provides a summary of IBM security bulletins, updates, and other product security related publications released between October and December 2011. The noted severity ratings follow the NIST guidelines for determining the severity rating based on the CVSS Base Score – see "**NVD Vulnerability Severity Ratings**" for details. In cases where a Security Bulletin or Update addresses more than one vulnerability, the highest CVSS Base Score is used to determine the overall severity.

For a current list of security bulletins, please visit the IBM Product Security Incident Response blog at **https://www.ibm.com/blogs/PSIRT**.

October 2011

Title: Vulnerability in Rational AppScan Standard, Express, Enterprise and Reporting Console with potential for command execution
Severity: High
CVE(s): CVE-2011-1366, CVE-2011-1367
Affected product(s): Rational AppScan Standard, Rational AppScan Enterprise, Rational AppScan Reporting Console
Affected version(s): 5.2 through 8.0.1
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21515110

Title: IBM WebSphere ILOG Rule Team Server home.jsp cross-site scripting
Severity: Medium
CVE(s): CVE-2011-4171
Affected product(s): IBM WebSphere ILOG Rule Team Server
Affected version(s): 7.1.1
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg1RS00803

Title: Fixes for security vulnerabilities in IBM Lotus Notes file viewers when viewing Ichitaro documents
Severity: High
CVE(s): CVE-2011-0337, CVE-2011-0338, CVE-2011-0339
Affected product(s): IBM Lotus Notes
Affected version(s): 8.0.2, 8.5, 8.5.1, 8.5.2
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21566925

Title: IBM WebSphere ILOG Rule Team Server error.jsp cross-site scripting
Severity: Medium
CVE(s): CVE-2011-1371
Affected product(s): IBM WebSphere ILOG Rule Team Server
Affected version(s): 7.1.1
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg1RS00810

Title: Potential Security Exposure in IBM Lotus Sametime Configuration Servlet
Severity: Medium
CVE(s): CVE-2011-1370
Affected product(s): IBM Lotus Sametime
Affected version(s): 7.0, 7.5, 7.5.1, 7.5.1.1, 7.5.1.2, 8.0, 8.0.1, 8.0.2, 8.5, 8.5.1, 8.5.1.1, 8.5.2
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21569452

Title: IBM DB2 Potential crash with STMM enabled and DATABASE_MEMORY set to Automatic
Severity: Low
CVE(s): CVE-2011-1373
Affected product(s): IBM DB2 for Linux, UNIX and Windows
Affected version(s): 9.7
Reference: https://www-304.ibm.com/support/docview.wss?uid=swg21450666 (APAR IC70473)

November 2011

Title: IBM DB2 Tools for z/OS Directory Browsing Vulnerability in CAE Server
Severity: Medium
CVE(s): CVE-2011-4435
Affected product(s): IBM DB2 Tools for z/OS
Affected version(s): 2.3.0
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg1PM41190

Title: IBM AIX - Multiple OpenSSL vulnerabilities
Severity: High
CVE(s): CVE-2010-3864, CVE-2010-4180, CVE-2011-0014
Affected product(s): IBM AIX
Affected version(s): 5.3, 6.1, 7.1

Reference:
http://aix.software.ibm.com/aix/efixes/security/openssl_advisory2.asc

Title: IBM Rational Asset Manager security bypass
Severity: Medium
CVE(s): CVE-2011-4820
Affected product(s): IBM Rational Asset Manager
Affected version(s): 7.5
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg1PM38335

Title: IBM Rational Asset Manager cross-site scripting
Severity: Medium
CVE(s): CVE-2011-4708
Affected product(s): IBM Rational Asset Manager
Affected version(s): 7.5
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg1PM38467

Title: IBM Lotus Domino remedy for BEAST Secure Socket Layer (SSL) 3.0 exploit recently published
Severity: Medium
CVE(s): CVE-2011-3389
Affected product(s): IBM Lotus Domino
Affected version(s): 8.0, 8.5, 8.5.1, 8.5.2, 8.5.3
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21568229

Title: IBM WebSphere MQ control commands security bypass
Severity: Low
CVE(s): CVE-2011-1378
Affected product(s): IBM WebSphere MQ
Affected version(s): 6.0
Reference: http://xforce.iss.net/xforce/xfdb/71336

Title: IBM AIX WPAR specific system call vulnerability
Severity: Medium
CVE(s): CVE-2011-1375
Affected product(s): IBM AIX
Affected version(s): 6.1, 7.1
Reference:
http://aix.software.ibm.com/aix/efixes/security/wpar_advisory.asc

Title: Vulnerability in the TS3100/TS3200 Web User Interface could allow unauthorized library access
Severity: Medium

CVE(s): CVE-2011-1372
Affected product(s): TS3100 and TS3200 tape libraries
Affected version(s): firmware versions below A.60
Reference: http://www-01.ibm.com/support/docview.wss?uid=ssg1S1003938

Title: IBM SDK for Java version 5.0 Service Refresh 13
Severity: High
CVE(s): CVE-2011-3545, CVE-2011-3547, CVE-2011-3548, CVE-2011-3549, CVE-2011-3552, CVE-2011-3554, CVE-2011-3556
Affected product(s): IBM SDK for Java
Affected version(s): 5.0
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21567199

Title: IBM AIX Perl Digest Module "Digest->new()" Code Injection Vulnerability
Severity: High
CVE(s): CVE-2011-3597
Affected product(s): IBM AIX
Affected version(s): 5.3, 6.1, 7.1
Reference:
http://aix.software.ibm.com/aix/efixes/security/perl_advisory2.asc

Title: IBM Tivoli Netcool/Reporter Apache CGI generic command execution vulnerability
Severity: High
CVE(s): CVE-2011-4668
Affected product(s): IBM Tivoli Netcool/Reporter
Affected version(s): 2.2
Reference: https://www-304.ibm.com/support/docview.wss?uid=swg24031456 (IZ94277-813)

December 2011

Title: Fix list for IBM solidDB V6.5 and IBM solidDB Universal Cache V6.5
Severity: Medium
CVE(s): CVE-2010-4055, CVE-2010-4056, CVE-2010-4057
Affected product(s): IBM solidDB, IBM solidDB Universal Cache
Affected version(s): 6.5
Reference: https://www-304.ibm.com/support/docview.wss?uid=swg27021052 (IC80074, IC80075, IC80076)

Title: IBM AIX inventory scout file deletion and symlink vulnerability
Severity: Medium

CVE(s): CVE-2011-1384
Affected product(s): IBM AIX
Affected version(s): 5.3, 6.1, 7.1
Reference:
http://aix.software.ibm.com/aix/efixes/security/invscout_advisory2.asc

Title: IBM Tivoli Federated Identity Manager SAML (Security Assertion Markup Language) non-conformance vulnerability
Severity: Medium
CVE(s): CVE-2011-1386
Affected product(s): IBM Tivoli Federated Identity Manager
Affected version(s): 6.1.1, 6.2.0, 6.2.1
Reference: https://www-304.ibm.com/support/docview.wss?uid=swg21575309

Title: IBM AIX - Multiple vulnerabilities in the X server
Severity: High
CVE(s): CVE-2007-6427, CVE-2007-6429
Affected product(s): IBM AIX
Affected version(s): 6.1, 7.1
Reference:
http://aix.software.ibm.com/aix/efixes/security/xorg_advisory.asc

Title: Potential Oracle Outside In Technology Vulnerabilities Exposed in ECM Products
Severity: High
CVE(s): CVE-2011-2264, CVE-2011-0794, CVE-2011-0808
Affected product(s): See Reference
Affected version(s): See Reference
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21574454

Title: Security vulnerability fixes: IBM Java Secure Socket Extension (IBMJSSE2)
Severity: Medium
CVE(s): CVE-2011-3389, CVE-2011-3560
Affected product(s): IBM SDK for Java
Affected version(s): 1.4.2, 6.0
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21571596

Title: Lotus Domino Denial of Service Vulnerability During Notes Authentication Processing
Severity: High
CVE(s): CVE-2011-1393
Affected product(s): IBM Lotus Domino

Affected version(s): 8.5.2 FP3 and prior, 8.5.1, 8.5, 8.0.x
Reference: http://www.ibm.com/support/docview.wss?uid=swg21575247

Title: IBM DB2 Escalation of Privilege Vulnerability
Severity: Medium
CVE(s): CVE-2011-4061
Affected product(s): IBM DB2
Affected version(s): 9.5, 9.7
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21576372

Title: Rational Rhapsody for Windows Blueberry FlashBack ActiveX Control Vulnerabilities
Severity: High
CVE(s): CVE-2011-1388, CVE-2011-1391, CVE-2011-1392
Affected product(s): IBM Rational Rhapsody
Affected version(s): 7.5.x, 7.6
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21576352

Title: IBM Web Experience Factory cross-site scripting
Severity: Medium
CVE(s): CVE-2011-5048
Affected product(s): IBM Web Experience Factory
Affected version(s): 7.0, 7.0.1
Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21575083

Title: Multiple Vulnerabilities in AIX BIND
Severity: Medium
CVE(s): CVE-2009-0025, CVE-2010-0097, CVE-2010-0382, CVE-2011-4313
Affected product(s): IBM AIX
Affected version(s): 5.3, 6.1, 7.1
Reference:
http://aix.software.ibm.com/aix/efixes/security/bind9_advisory3.asc

Note: *According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.*