



CVE-2014-3095

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2014-3095 |
| State | PUBLIC |
| Assigner | psirt@us.ibm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2014-09-04 10:55:00 UTC |
| Updated | 2017-08-29 01:34:00 UTC |
| Description | The SQL engine in IBM DB2 9.5 through FP10, 9.7 through FP9a, 9.8 through FP5, 10.1 through FP4, and 10.5 before FP4 |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|----------|--------|---------|----------|
| Application | ibm | Db2 | 10.1 | All | All | All |
| Application | ibm | Db2 | 10.1.0.1 | All | All | All |
| Application | ibm | Db2 | 10.1.0.2 | All | All | All |
| Application | ibm | Db2 | 10.1.0.3 | All | All | All |
| Application | ibm | Db2 | 10.1.0.3 | a | All | All |
| Application | ibm | Db2 | 10.1.0.4 | All | All | All |
| Application | ibm | Db2 | 10.5 | All | All | All |
| Application | ibm | Db2 | 10.5.0.1 | All | All | All |
| Application | ibm | Db2 | 10.5.0.2 | All | All | All |
| Application | ibm | Db2 | 10.5.0.3 | All | All | All |
| Application | ibm | Db2 | 10.5.0.3 | a | All | All |
| Application | ibm | Db2 | 9.5 | All | All | All |
| Application | ibm | Db2 | 9.5.0.1 | All | All | All |
| Application | ibm | Db2 | 9.5.0.10 | All | All | All |
| Application | ibm | Db2 | 9.5.0.2 | All | All | All |
| Application | ibm | Db2 | 9.5.0.2 | a | All | All |
| Application | ibm | Db2 | 9.5.0.3 | All | All | All |

| | | | | | | |
|-------------|-----|-----|----------|-----|-----|-----|
| Application | lbn | Db2 | 9.5.0.3 | a | All | All |
| Application | lbn | Db2 | 9.5.0.3 | b | All | All |
| Application | lbn | Db2 | 9.5.0.4 | All | All | All |
| Application | lbn | Db2 | 9.5.0.4 | a | All | All |
| Application | lbn | Db2 | 9.5.0.5 | All | All | All |
| Application | lbn | Db2 | 9.5.0.6 | a | All | All |
| Application | lbn | Db2 | 9.5.0.7 | All | All | All |
| Application | lbn | Db2 | 9.5.0.8 | All | All | All |
| Application | lbn | Db2 | 9.5.0.9 | All | All | All |
| Application | lbn | Db2 | 9.7 | All | All | All |
| Application | lbn | Db2 | 9.7.0.1 | All | All | All |
| Application | lbn | Db2 | 9.7.0.2 | All | All | All |
| Application | lbn | Db2 | 9.7.0.3 | All | All | All |
| Application | lbn | Db2 | 9.7.0.4 | All | All | All |
| Application | lbn | Db2 | 9.7.0.5 | All | All | All |
| Application | lbn | Db2 | 9.7.0.6 | All | All | All |
| Application | lbn | Db2 | 9.7.0.7 | All | All | All |
| Application | lbn | Db2 | 9.7.0.8 | All | All | All |
| Application | lbn | Db2 | 9.7.0.9 | All | All | All |
| Application | lbn | Db2 | 9.7.0.9 | a | All | All |
| Application | lbn | Db2 | 9.8 | All | All | All |
| Application | lbn | Db2 | 9.8.0.3 | All | All | All |
| Application | lbn | Db2 | 9.8.0.4 | All | All | All |
| Application | lbn | Db2 | 9.8.0.5 | All | All | All |
| Application | lbn | Db2 | 10.1 | All | All | All |
| Application | lbn | Db2 | 10.1.0.1 | All | All | All |
| Application | lbn | Db2 | 10.1.0.2 | All | All | All |
| Application | lbn | Db2 | 10.1.0.3 | All | All | All |
| Application | lbn | Db2 | 10.1.0.3 | a | All | All |
| Application | lbn | Db2 | 10.1.0.4 | All | All | All |
| Application | lbn | Db2 | 10.5 | All | All | All |
| Application | lbn | Db2 | 10.5.0.1 | All | All | All |
| Application | lbn | Db2 | 10.5.0.2 | All | All | All |
| Application | lbn | Db2 | 10.5.0.3 | All | All | All |
| Application | lbn | Db2 | 10.5.0.3 | a | All | All |

| | | | | | | |
|------------------|-----------|--------------|----------|-----|-----|-----|
| Application | IBM | Db2 | 9.5 | All | All | All |
| Application | IBM | Db2 | 9.5.0.1 | All | All | All |
| Application | IBM | Db2 | 9.5.0.10 | All | All | All |
| Application | IBM | Db2 | 9.5.0.2 | All | All | All |
| Application | IBM | Db2 | 9.5.0.2 | a | All | All |
| Application | IBM | Db2 | 9.5.0.3 | All | All | All |
| Application | IBM | Db2 | 9.5.0.3 | a | All | All |
| Application | IBM | Db2 | 9.5.0.3 | b | All | All |
| Application | IBM | Db2 | 9.5.0.4 | All | All | All |
| Application | IBM | Db2 | 9.5.0.4 | a | All | All |
| Application | IBM | Db2 | 9.5.0.5 | All | All | All |
| Application | IBM | Db2 | 9.5.0.6 | a | All | All |
| Application | IBM | Db2 | 9.5.0.7 | All | All | All |
| Application | IBM | Db2 | 9.5.0.8 | All | All | All |
| Application | IBM | Db2 | 9.5.0.9 | All | All | All |
| Application | IBM | Db2 | 9.7 | All | All | All |
| Application | IBM | Db2 | 9.7.0.1 | All | All | All |
| Application | IBM | Db2 | 9.7.0.2 | All | All | All |
| Application | IBM | Db2 | 9.7.0.3 | All | All | All |
| Application | IBM | Db2 | 9.7.0.4 | All | All | All |
| Application | IBM | Db2 | 9.7.0.5 | All | All | All |
| Application | IBM | Db2 | 9.7.0.6 | All | All | All |
| Application | IBM | Db2 | 9.7.0.7 | All | All | All |
| Application | IBM | Db2 | 9.7.0.8 | All | All | All |
| Application | IBM | Db2 | 9.7.0.9 | All | All | All |
| Application | IBM | Db2 | 9.7.0.9 | a | All | All |
| Application | IBM | Db2 | 9.8 | All | All | All |
| Application | IBM | Db2 | 9.8.0.3 | All | All | All |
| Application | IBM | Db2 | 9.8.0.4 | All | All | All |
| Application | IBM | Db2 | 9.8.0.5 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Microsoft | Windows | All | All | All | All |
| Operating System | Microsoft | Windows | All | All | All | All |

| Reference |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IT02643 |
| IBM IT02645: SECURITY: DB2 contains a denial of service vulnerability in SQL Compiler (CVE-2014-3095) - United States |
| About Secunia Research Flexera |
| IBM X-Force Exchange |
| IBM Security Bulletin: IBM® DB2® LUW contains a denial of service vulnerability using a SELECT statement with a subquery containing a UN |
| Security Bulletin: IBM® InfoSphere Balanced Warehouse, IBM Smart Analytics System and IBM PureData System for Operational Analytics a |
| IT02644 |
| Multiple IBM DB2 Products CVE-2014-3095 Remote Denial of Service Vulnerability |
| IT02433: SECURITY: DB2 contains a denial of service vulnerability in SQL Compiler (CVE-2014-3095) |
| IBM IT02646: SECURITY: DB2 contains a denial of service vulnerability in SQL Compiler (CVE-2014-3095) - United States |
| Security Advisory SA60845 - IBM DB2 / DB2 Connect Multiple Vulnerabilities - Secunia |
| CVE Program record |
| NVD vulnerability detail |
| <div style="border: 1px solid #ccc; height: 15px; width: 100%; background-color: #f0f0f0; position: relative;"> <div style="position: absolute; left: -10px; top: 5px;">◀</div> <div style="position: absolute; right: -10px; top: 5px;">▶</div> </div> |
| No vendor comments have been submitted for this CVE. |
| There are currently no legacy QID mappings associated with this CVE. |

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report