



# CVE-2010-1041

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-1041                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | cve@mitre.org                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2010-03-23 00:53:00 UTC                                                                                                     |
| <b>Updated</b>         | 2010-06-11 04:00:00 UTC                                                                                                     |
| <b>Description</b>     | Unspecified vulnerability in the single sign-on functionality in the Web Services implementation in IBM DB2 Content Manager |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product             | Version | Update | Edition | Language |
|-------------|--------|---------------------|---------|--------|---------|----------|
| Application | ibm    | Db2 Content Manager | 8.3     | All    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp1    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp10   | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp11   | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp2    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp3    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp3a   | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp4    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp5    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp6    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp7    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp8    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp9    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | All    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp1    | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp10   | All     | All      |
| Application | ibm    | Db2 Content Manager | 8.3     | fp11   | All     | All      |

|             |                     |                                     |     |      |     |     |
|-------------|---------------------|-------------------------------------|-----|------|-----|-----|
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp2  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp3  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp3a | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp4  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp5  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp6  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp7  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp8  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | 8.3 | fp9  | All | All |
| Application | <a href="#">Ibm</a> | <a href="#">Db2 Content Manager</a> | All | fp12 | All | All |

| References                                                                                                     |         |                       |
|----------------------------------------------------------------------------------------------------------------|---------|-----------------------|
| Reference                                                                                                      | Source  | Link                  |
| IBM notice: The page you requested cannot be displayed                                                         | CONFIRM | <a href="#">www</a>   |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                               | VUPEN   | <a href="#">www</a>   |
| 63079                                                                                                          | OSVDB   | <a href="#">www</a>   |
| IBM notice: The page you requested cannot be displayed                                                         | AIXAPAR | <a href="#">www</a>   |
| IBM DB2 Content Manager Information Integrator Security Issue - Advisories - Community                         | SECUNIA | <a href="#">secu</a>  |
| IBM PM03804: CM Z/OS 8.3 TOOLKIT FIX PACK 13 ROLL-UP PTF - United States                                       | AIXAPAR | <a href="#">www</a>   |
| IBM DB2 Content Manager Web Services Unspecified Vulnerability                                                 | BID     | <a href="#">www</a>   |
| SecurityTracker.com Archives - IBM DB2 Content Manager Web Services Single Sign-on Flaw Has Unspecified Impact | SECTRAK | <a href="#">secu</a>  |
| CVE Program record                                                                                             | CVE.ORG | <a href="#">www</a>   |
| NVD vulnerability detail                                                                                       | NVD     | <a href="#">nvd.i</a> |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.