



# CVE-2017-1520

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-1520                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | psirt@us.ibm.com                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2017-09-12 21:29:00 UTC                                                                                                  |
| <b>Updated</b>         | 2017-09-15 19:05:00 UTC                                                                                                  |
| <b>Description</b>     | IBM DB2 9.7, 10,1, 10.5, and 11.1 is vulnerable to an unauthorized command that allows the database to be activated when |

## Risk And Classification

### Problem Types: CWE-287

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor              | Product             | Version  | Update | Edition | Language |
|-------------|---------------------|---------------------|----------|--------|---------|----------|
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.1     | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.1.0.1 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.1.0.2 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.1.0.3 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.1.0.4 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.1.0.5 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5     | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.1 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.2 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.3 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.3 | a      | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.4 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.5 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.6 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 10.5.0.7 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 11.1.0.0 | All    | All     | All      |
| Application | <a href="#">Ibm</a> | <a href="#">Db2</a> | 9.7      | All    | All     | All      |

|             |     |     |          |     |     |     |
|-------------|-----|-----|----------|-----|-----|-----|
|             |     |     |          |     |     |     |
| Application | lbn | Db2 | 9.7.0.1  | All | All | All |
| Application | lbn | Db2 | 9.7.0.10 | All | All | All |
| Application | lbn | Db2 | 9.7.0.11 | 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 | 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 | 10.1.0.4 | All | All | All |
| Application | lbn | Db2 | 10.1.0.5 | 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 | lbn | Db2 | 10.5.0.4 | All | All | All |
| Application | lbn | Db2 | 10.5.0.5 | All | All | All |
| Application | lbn | Db2 | 10.5.0.6 | All | All | All |
| Application | lbn | Db2 | 10.5.0.7 | All | All | All |
| Application | lbn | Db2 | 11.1.0.0 | All | All | All |
| Application | lbn | Db2 | 9.7      | All | All | All |
| Application | lbn | Db2 | 9.7.0.1  | All | All | All |
| Application | lbn | Db2 | 9.7.0.10 | All | All | All |
| Application | lbn | Db2 | 9.7.0.11 | 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      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.1.0.2 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.1.0.3 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.1.0.4 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.1.0.5 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5     | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.1 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.2 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.3 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.4 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.5 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.6 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 10.5.0.7 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 11.1.0.0 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7      | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.1  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.10 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.11 | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.2  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.3  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.4  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.5  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.6  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.7  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.8  | All | All | All |
| Application      | <a href="#">Ibm</a>       | <a href="#">Db2 Connect</a>  | 9.7.0.9  | All | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | -        | All | All | All |
| Operating System | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | -        | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows</a>      | -        | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows</a>      | -        | All | All | All |

References

Reference

IBM DB2 CLIENT Authentication Flaw Lets Remote Users Activate the Target Database - SecurityTracker

Security Bulletin: IBM® Db2® is vulnerable to an unauthorized command that allows the database to be activated when authentication type is

IBM X-Force Exchange

IBM DB2 CVE-2017-1520 Security Bypass Vulnerability

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)