



CVE-2020-4739

Published on: 11/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:23 PM UTC

CVE-2020-4739

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **Db2** from **ibm** contain the following vulnerability:

IBM DB2 Accessories Suite for Linux, UNIX, and Windows, DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 188149.

CVE-2020-4739 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **DB2 for Linux, UNIX and Windows** version **10.5**

Affected Vendor/Software: [IBM](#) - **DB2 for Linux, UNIX and Windows** version **10.1**

Affected Vendor/Software: [IBM](#) - **DB2 for Linux, UNIX and Windows** version **9.7**

Affected Vendor/Software: [IBM](#) - **DB2 for Linux, UNIX and Windows** version **11.1**

Affected Vendor/Software: [IBM](#) - **DB2 for Linux, UNIX and Windows** version **11.5**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE

Confidentiality Impact

Integrity Impact

Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Security Bulletin: IBM® Db2® could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. (CVE-2020-4739)

Patch

Vendor Advisory

www.ibm.com

text/html

 CONFIRM

www.ibm.com/support/pages/node/6370023

IBM X-Force Exchange

VDB Entry

Vendor Advisory

web.archive.org

text/html

Inactive Link

Not Archived

 XF ibm-db2-cve20204739-code-exec (188149)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

375925 IBM Spectrum Protect Server Multiple Vulnerabilities (6446749)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	IBM	Db2	All	All	All	All
Application	IBM	Db2	10.1.0.0	All	All	All
Application	IBM	Db2	10.5.0.0	All	All	All
Application	IBM	Db2	11.1.0.0	All	All	All
Application	IBM	Db2	9.7.0.0	All	All	All
Application	IBM	Db2	All	All	All	All
Application	IBM	Db2	10.1.0.0	All	All	All
Application	IBM	Db2	10.5.0.0	All	All	All
Application	IBM	Db2	11.1.0.0	All	All	All
Application	IBM	Db2	9.7.0.0	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:ibm:db2:*.~.*

cpe:2.3:a:ibm:db2:10.5.0.0:*****:
cpe:2.3:a:ibm:db2:11.1.0.0:*****:
cpe:2.3:a:ibm:db2:9.7.0.0:*****:
cpe:2.3:a:ibm:db2:*****:
cpe:2.3:a:ibm:db2:10.1.0.0:*****:
cpe:2.3:a:ibm:db2:10.5.0.0:*****:
cpe:2.3:a:ibm:db2:11.1.0.0:*****:
cpe:2.3:a:ibm:db2:9.7.0.0:*****:
cpe:2.3:o:microsoft:windows:-:*****:
cpe:2.3:o:microsoft:windows:-:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @L2clrogers	Security Bulletin: Vulnerabilities in IBM Db2 affect the IBM Spectrum Protect Server (CVE-2020-4701, CVE-2020-4739)... twitter.com/i/web/status/1...	2021-05-30 01:13:58

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

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