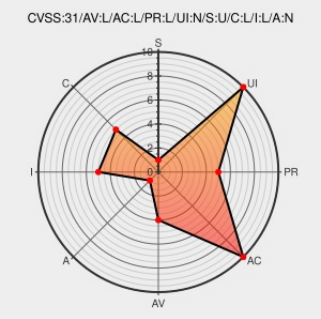
CVE-2020-4976

Published on: 03/11/2021 12:00:00 AM UTC

Last Modified on: 04/12/2021 04:41:00 PM UTC

CVE-2020-4976

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Db2 from Ibm contain the following vulnerability:

IBM 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 user to read and write specific files due to weak file permissions. IBM X-Force ID: 192469.

CVE-2020-4976 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as MEDIUM 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: 4.4 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | NONE

CVE References

Description	Tags	Link
March 2021 IBM DB2 Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20210409-0003/
Security Bulletin: IBM® Db2® is vulnerable to weak file permissions allowing access to specific files (CVE-2020-4976)	Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6427859
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-db2-cve20204976-file-write (192469)

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

375635 IBM Spectrum Protect Server Multiple Vulnerabilities (6462189)

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	-	All	All
Application	Ibm	Db2	10.1	fp1	All	All
Application	Ibm	Db2	10.1	fp2	All	All
Application	Ibm	Db2	10.1	fp3	All	All
Application	Ibm	Db2	10.1	fp3a	All	All
Application	Ibm	Db2	10.1	fp4	All	All
Application	Ibm	Db2	10.1	fp5	All	All
Application	Ibm	Db2	10.5	-	All	All
Application	Ibm	Db2	10.5	fp1	All	All
Application	Ibm	Db2	10.5	fp2	All	All
Application	Ibm	Db2	10.5	fp3	All	All
Application	Ibm	Db2	10.5	fp3a	All	All
Application	Ibm	Db2	10.5	fp4	All	All
Application	Ibm	Db2	10.5	fp5	All	All
Application	Ibm	Db2	10.5	fp6	All	All
Application	Ibm	Db2	10.5	fp7	All	All

Application	Ibm	Db2	10.5	fp8	All	All
Application	Ibm	Db2	10.5	fp9	All	All
Application	Ibm	Db2	9.7	-	All	All
Application	Ibm	Db2	9.7	fp1	All	All
Application	Ibm	Db2	9.7	fp10	All	All
Application	Ibm	Db2	9.7	fp2	All	All
Application	Ibm	Db2	9.7	fp3	All	All
Application	Ibm	Db2	9.7	fp3a	All	All
Application	Ibm	Db2	9.7	fp4	All	All
Application	Ibm	Db2	9.7	fp5	All	All
Application	Ibm	Db2	9.7	fp6	All	All
Application	Ibm	Db2	9.7	fp7	All	All
Application	Ibm	Db2	9.7	fp8	All	All
Application	Ibm	Db2	9.7	fp9	All	All
Application	Ibm	Db2	9.7	fp9a	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All

cpe:2.3:a:ibm:db2:*:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:-:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.1:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:-:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp6:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp7:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp8:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5:fp9:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:-:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp1:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp10:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp2:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp3:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp3a:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp4:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp5:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp6:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp7:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp8:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp9:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7:fp9a:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:oncommand_insight:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← 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 registred 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