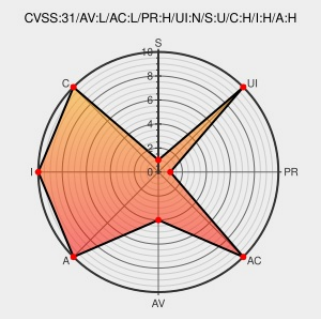
CVE-2019-4057

Published on: 07/01/2019 12:00:00 AM UTC

Last Modified on: 12/09/2022 04:11:00 PM UTC

CVE-2019-4057

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, and 11.1 could allow malicious user with access to the DB2 instance account to leverage a fenced execution process to execute arbitrary code as root. IBM X-Force ID: 156567.

CVE-2019-4057 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**

CVSS3 Score: 6.7 - MEDIUM

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

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	XF ibm-db2-cve20194057-priv-escalation (156567)
Security Bulletin: IBM® Db2® is vulnerable to privilege escalation to root via malicious use of fenced user (CVE-2019-4057).	Vendor Advisory www.ibm.com text/html	CONFIRM www.ibm.com/support/docview.wss?uid=ibm10880735

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Db2	10.1.0.0	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	10.1.0.4	All	All	All
Application	Ibm	Db2	10.1.0.5	All	All	All
Application	Ibm	Db2	10.1.0.6	All	All	All
Application	Ibm	Db2	10.5.0.0	All	All	All
Application	Ibm	Db2	10.5.0.1	All	All	All
Application	Ibm	Db2	10.5.0.10	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	10.5.0.4	All	All	All
Application	Ibm	Db2	10.5.0.5	All	All	All
Application	Ibm	Db2	10.5.0.6	All	All	All
Application	Ibm	Db2	10.5.0.7	All	All	All
Application	Ibm	Db2	10.5.0.8	All	All	All
Application	Ibm	Db2	10.5.0.9	All	All	All
Application	Ibm	Db2	11.1.0.0	All	All	All
Application	Ibm	Db2	11.1.1.1	All	All	All
Application	Ibm	Db2	11.1.2.2	All	All	All

Application	Ibm	Db2	11.1.3.3	All	All	All
Application	Ibm	Db2	11.1.4.4	All	All	All
Application	Ibm	Db2	9.7.0.0	All	All	All
Application	Ibm	Db2	9.7.0.1	All	All	All
Application	Ibm	Db2	9.7.0.10	All	All	All
Application	Ibm	Db2	9.7.0.11	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	10.1.0.0	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	10.1.0.4	All	All	All
Application	Ibm	Db2	10.1.0.5	All	All	All
Application	Ibm	Db2	10.1.0.6	All	All	All
Application	Ibm	Db2	10.5.0.0	All	All	All
Application	Ibm	Db2	10.5.0.1	All	All	All
Application	Ibm	Db2	10.5.0.10	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	10.5.0.4	All	All	All
Application	Ibm	Db2	10.5.0.5	All	All	All
Application	Ibm	Db2	10.5.0.6	All	All	All
Application	Ibm	Db2	10.5.0.7	All	All	All
Application	Ibm	Db2	10.5.0.8	All	All	All
Application	Ibm	Db2	10.5.0.9	All	All	All
Application	Ibm	Db2	11.1.0.0	All	All	All
Application	Ibm	Db2	11.1.1.1	All	All	All
Application	Ibm	Db2	11.1.2.2	All	All	All

Application	Ibm	Db2	11.1.3.3	All	All	All
Application	Ibm	Db2	11.1.4.4	All	All	All
Application	Ibm	Db2	9.7.0.0	All	All	All
Application	Ibm	Db2	9.7.0.1	All	All	All
Application	Ibm	Db2	9.7.0.10	All	All	All
Application	Ibm	Db2	9.7.0.11	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
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:ibm:db2:10.1.0.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.4:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.5:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.6:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.10:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.4:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.5:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.6:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.7:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.8:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.5.0.9:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:11.1.0.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:11.1.1.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:11.1.2.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:11.1.3.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:11.1.4.4:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.10:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.11:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.4:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.5:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.6:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.7:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.8:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:9.7.0.9:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.0:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.1:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.4:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.5:*:*:*:*:*:*:*

cpe:2.3:a:ibm:db2:10.1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:10.5.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:11.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:11.1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:11.1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:11.1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:11.1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:db2:9.7.0.9:*:*:*:*:*:*:*

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→