



Security Bulletin: IBM® Db2® is vulnerable to a denial of service with a specially crafted query involving multiple subqueries (CVE-2026-1577)

Security Bulletin

Summary

IBM® Db2® is vulnerable to a denial of service with a specially crafted query involving multiple subqueries.

Vulnerability Details

CVEID: [CVE-2026-1577](https://www.cve.org/CVERecord?id=CVE-2026-1577) (<https://www.cve.org/CVERecord?id=CVE-2026-1577>)

DESCRIPTION: IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow

an authenticated user to cause a denial of service due to improper neutralization of special elements in data ✕

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising.

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes. This activity may qualify as a "sale" or "sharing" under the California

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).

Accept all

Do not sell or share my personal information

Product(s)	Version(s)	Applicable Editions
IBM Db2 for Linux, UNIX and Windows	11.5.9 - 11.5.9	Server
IBM Db2 for Linux, UNIX and Windows	12.1.0 - 12.1.4	Server

For more information, please review your [cookie preferences](#) options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#)

(<https://www.ibm.com/us-en/privacy/ccp>)
Customers running any vulnerable affected level of an affected Program, V11.5, and V12.1, can download the special build containing the interim fix for this issue from Fix Central. These special builds are available based

on the most recent level for each impacted release: V11.5.9, and V12.1.4. They can be applied to any affected level of the appropriate release to remediate this vulnerability.

Release	Fixed in mod pack	APAR	Download URL
V11.5	TBD	DT460939 (https://www.ibm.com/mysupport/s/defect/aClgJ0000009d3l/dt460939)	Special Build #79671 or later for V11.5.9 available at this link: https://www.ibm.com/support/pages/node/7087189 (https://www.ibm.com/support/pages/node/7087189)
V12.1	TBD	DT460939 (https://www.ibm.com/mysupport/s/defect/aClgJ0000009d3l/dt460939)	Special Build #80714 or later for V12.1.4 available at this link: https://www.ibm.com/support/pages/node/7267513 (https://www.ibm.com/support/pages/node/7267513)

About cookies on this site

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising. For more information, please review your options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](https://www.ibm.com/us-en/privacy/ccpa) (<https://www.ibm.com/us-en/privacy/ccpa>)

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes. This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act "CCPA". By selecting "Do not sell or share my personal information", you are requesting IBM to use required cookies only.

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).



Published Security Vulnerabilities for DB2 for Linux, UNIX, and Windows including Special Build information

(<https://www.ibm.com/support/pages/published-security-vulnerabilities-db2-linux-unix-and-windows-including-special-build-information>)

Acknowledgement

Change History

15 Apr 2026: Initial Publication

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring

System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine X

urgency of response." IBM PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF

ANY INCLUSIONS, EXCLUSIONS, OR WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY

ACTUAL POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential

vulnerabilities, IBM periodically updates the components contained in our product offerings. As part of

that process, IBM periodically updates the components in a product/service inventory, we address relevant

vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced

product has been used at that date, nor that IBM was aware of a vulnerability as of that date. We are

not aware of any vulnerabilities as we become aware of them. "Affected Products and Versions"

reference is intended to be only products and versions that are supported by IBM

at the time of publication of this Security Bulletin does not constitute a determination by IBM that they are

supported or extended-supported. Reference to one or more unsupported versions in this Security Bulletin shall not

constitute a determination by IBM that they are supported or extended-supported for any unsupported or extended-support products or versions.

options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#)

1) (<https://www.ibm.com/us-en/privacy/ccp>)

Operating system(s):

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Linux, Linux on IBM Z Systems, AIX, Windows

Document number:

7269434

Modified date:

15 April 2026

Initial Publish date:

15 April 2026

**About cookies on this site**

Our websites require some cookies to function properly (required). In addition, other cookies may be used with your consent to analyze site usage, improve the user experience and for advertising. For more information, please review your

options. By visiting our website, you agree to our processing of information as described in IBM's [privacy statement](#)

(<https://www.ibm.com/us-en/privacy/ccpa>)

In addition to the services they provide to IBM, certain IBM authorized partners may also use these cookies for their own purposes. This activity may qualify as a "sale" or "sharing" under the California Consumer Privacy Act "CCPA". By selecting "Do not sell or share my personal information", you are requesting IBM to use required cookies only.

To provide a smooth navigation, your cookie preferences will be shared across the IBM web domains listed [here](#).