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)*

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 query logic.

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/aCIgJ0000009d3l/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/aCIgJ0000009d3l/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)*

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 urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the versions of components contained in our product offerings. As part of that effort, IBM identifies vulnerabilities by unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE ID date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM as of that date, nor that IBM was aware of a vulnerability as of that date. We are making efforts to become aware of vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in this Security Bulletin are intended to be only products and versions that are supported by IBM and have not passed the end of support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected. Reference to one or more unsupported versions in this Security Bulletin shall not create an expectation that fixes for any unsupported or extended-support products or versions.

Document number:

7269434

Modified date:

15 April 2026

Initial Publish date:

15 April 2026