



Security Bulletin: IBM® Db2® is vulnerable to a denial of service under specific conditions (CVE-2024-52903)

Security Bulletin

Summary

IBM® Db2® is vulnerable to a denial of service under specific conditions with a specially crafted query.

Vulnerability Details

CVEID: [CVE-2024-52903](https://www.cve.org/CVERecord?id=CVE-2024-52903) (<https://www.cve.org/CVERecord?id=CVE-2024-52903>)

DESCRIPTION: IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.

CWE: [CWE-20: Improper Input Validation](https://cwe.mitre.org/data/definitions/20.html) (<https://cwe.mitre.org/data/definitions/20.html>)

CVSS Source: IBM

CVSS Base score: 5.3

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)	Applicable Editions
IBM® Db2®	12.1.0 - 12.1.1	Server

All platforms are affected.

Remediation/Fixes

Customers running any vulnerable affected level of an affected Program, 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: V12.1. They can be applied to any affected level of the appropriate release to remediate this vulnerability.

Release	Fixed in fix pack	APAR	Download URL
V12.1	TBD	DT409052 (https://www.ibm.com/my support/s/defect/aCI/Ke000000CjkD/dt409052)	<p>Special Build #50594 or later for V12.1.0 available at this link: https://www.ibm.com/support/pages/node/7176384 (https://www.ibm.com/support/pages/node/7176384)</p> <p>Special Build #56931 or later for V12.1.1 available at this link: https://www.ibm.com/support/pages/db2-v1211-published-cumulative-special-build-downloads#52441 (https://www.ibm.com/support/pages/db2-v1211-published-cumulative-special-build-downloads#52441)</p>

IBM does not disclose key Db2 functionality nor replication steps for a vulnerability to avoid providing too much information to any potential malicious attacker. IBM does not want to enable a malicious attacker with sufficient knowledge to craft an exploit of the vulnerability.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

- Subscribe to [My Notifications](https://www.ibm.com/support/pages/node/718119) (<https://www.ibm.com/support/pages/node/718119>) to be notified of important product support alerts like this.

References

- [Complete CVSS v3 Guide](#) ↗
- [On-line Calculator v3](#) ↗

Related Information

- [IBM Secure Engineering Web Portal](http://www.ibm.com/security/secure-engineering/bulletins.html) (<http://www.ibm.com/security/secure-engineering/bulletins.html>)
- [IBM Product Security Incident Response Blog](http://www.ibm.com/blogs/psirt) (<http://www.ibm.com/blogs/psirt>)
- [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)
(<https://www.ibm.com/support/pages/published-security-vulnerabilities-db2-linux-unix-and-windows-including-special-build-information>)

Acknowledgement

Change History

01 May 2025: 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 record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages 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 by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their 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 by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Document Information

More support for:

[Db2 for Linux, UNIX and Windows](https://www.ibm.com/mysupport/s/topic/OTO500000001fUNGAY) (*https://www.ibm.com/mysupport/s/topic/OTO500000001fUNGAY*)

Software version:

12.1.0

Operating system(s):

Linux on IBM Z Systems, Linux, AIX, Windows

Document number:

7232336

Modified date:

