Security Bulletin: IBM® Db2® is vulnerable to a denial of service with a specially crafted query when stmtheap is set to automatic (CVE-2025-36122)

Security Bulletin

Summary

IBM® Db2® is vulnerable to a denial of service with a specially crafted query when stmtheap is set to AUTOMATIC(limit).

Vulnerability Details

CVEID: CVE-2025-36122 *(https://www.cve.org/CVERecord?id=CVE-2025-36122)*

DESCRIPTION: IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow an authenticated user to cause a denial of service using a specially crafted SQL query due to improper allocation of system resources.

CWE: CWE-770: Allocation of Resources Without Limits or Throttling *(https://cwe.mitre.org/data/definitions/770.html)*

CVSS Source: IBM

CVSS Base score: 6.5

CVSS Vector: (CVSS:3.1/AV:N/AC:L/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®	11.5.0 - 11.5.9	Client and Server
IBM® Db2®	12.1.0 - 12.1.3	Client and Server

All platforms are affected.

Earlier releases (11.1, 10.5, 10.1, 9.7 etc.) may also be affected, but they are no longer supported. Any older version not mentioned above is not supported.

Remediation/Fixes

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. 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	DT444599 *(https://www.ibm.com/mysupport/s/defect/aCIgJ0000002v3p/dt444599)*	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	V12.1.4	DT444599 *(https://www.ibm.com/mysupport/s/defect/aCIgJ0000002v3p/dt444599)*	Latest for V12.1.4 is available at this link: https://www.ibm.com/support/pages/node/7267513 *(https://www.ibm.com/support/pages/node/7267513)*

Note: To apply this fix, it is required to set DB2_STRICT_INSTANCE_MEMORY=ON in addition to installing the above Specia

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

set dbm cfg instance_memory to a fixed value

Get Notified about Future Security Bulletins

ⓘ Subscribe to My Notifications *(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)*

IBM Product Security Incident Response Blog *(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)*

Acknowledgement

Change History

16 Apr 2026: Updated Remediation/Fixes to specify DB2_STRICT_INSTANCE_MEMORY requirement
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

Document Information

More support for:

Db2 for Linux, UNIX and Windows *(https://www.ibm.com/mysupport/s/topic/0TO500000001fUNGAY)*

Software version:

11.5.9, 12.1.x

Operating system(s):

AIX, Linux, Linux on IBM Z Systems, Windows

Document number:

7267642

Modified date:

16 April 2026

Initial Publish date:

15 April 2026