



# 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) (<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) (<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	✕
-----------	-----------------	-------------------	---

**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 [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/privac>  
y)

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

Accept all

More options

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 ( <a href="https://www.ibm.com/my-support/s/defect/aClgJ000002v3p/dt444599">https://www.ibm.com/my-support/s/defect/aClgJ000002v3p/dt444599</a> )	Special Build #79671 or later for V11.5.9 available at this link: <a href="https://www.ibm.com/support/pages/node/7087189">https://www.ibm.com/support/pages/node/7087189</a> ( <a href="https://www.ibm.com/support/pages/node/7087189">https://www.ibm.com/support/pages/node/7087189</a> )
V12.1	V12.1.4	DT444599 ( <a href="https://www.ibm.com/my-support/s/defect/aClgJ000002v3p/dt444599">https://www.ibm.com/my-support/s/defect/aClgJ000002v3p/dt444599</a> )	Latest for V12.1.4 is available at this link: <a href="https://www.ibm.com/support/pages/node/7267513">https://www.ibm.com/support/pages/node/7267513</a> ( <a href="https://www.ibm.com/support/pages/node/7267513">https://www.ibm.com/support/pages/node/7267513</a> )

Note: To apply this fix, it is required to set DB2\_STRICT\_INSTANCE\_MEMORY=ON in addition to installing the above Special Build.

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



#### 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/privacy-statement) (<https://www.ibm.com/privacy-statement>)

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

### 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

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

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 unsupported or have passed their end-of-support or warranty date. IBM does not provide fixes for any unsupported products or versions. ✕

### 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/privacy) (<https://www.ibm.com/privacy>)

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

**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



**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/privacy) (<https://www.ibm.com/privacy>)

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