



IBM® Db2® is vulnerable to a denial of service with a specially crafted query when stmtheap is set to automatic

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-36122
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 22:16:24 UTC
Updated	2026-04-30 22:16:24 UTC
Description	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes DB2 Connect Server) co

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from psirt@us.ibm.com

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

Problem Types: CWE-770 | CWE-770 CWE-770 Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
3.1	psirt@us.ibm.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IBM	Db2	affected 11.5.0 11.5.9 semver	Not specified
CNA	IBM	Db2	affected 12.1.0 12.1.3 semver	Not specified

References

Reference	Source	Link	Tags
www.ibm.com/support/pages/node/7267642	psirt@us.ibm.com	www.ibm.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: 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. ReleaseFixed in mod packAPARDownload URLV11.5TBD

<https://www.ibm.com/support/pages/node/7087189> V12.1 V12.1.4

<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 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

CNA: set dbm cfg instance_memory to a fixed value

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)