



# PostgreSQL pg\_restore\_attribute\_stats accepts values that cause query planning to read past end of stats array

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-6575
<b>State</b>	PUBLISHED
<b>Assigner</b>	PostgreSQL
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-14 14:16:25 UTC
<b>Updated</b>	2026-05-14 16:21:23 UTC
<b>Description</b>	Buffer over-read in PostgreSQL function pg_restore_attribute_stats() accepts array values of unmatched length, which causes

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from f86ef6dc-4d3a-42ad-8f28-e6d5547a5007

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

**EPSS:** 0.000270000 probability, percentile 0.078990000 (date 2026-05-17)

**Problem Types:** CWE-126 | CWE-126 Buffer Over-read

Version	Source	Type	Score	Severity	Vector
3.1	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	PostgreSQL	affected 18 18.4 rpm	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.postgresql.org/support/security/CVE-2026-6575">www.postgresql.org/support/security/CVE-2026-6575</a>	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	<a href="http://www.postgresql.org">www.postgresql.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** The PostgreSQL project thanks Jeroen Gui for reporting this problem. (en)

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

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

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)