



# PostgreSQL pg\_basebackup and pg\_rewind can overwrite unrelated files of origin superuser choice

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

## Summary

<b>CVE</b>	CVE-2026-6475
<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>	Symlink following in PostgreSQL pg_basebackup plain format and in pg_rewind allows an origin superuser to overwrite loca

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from f86ef6dc-4d3a-42ad-8f28-e6d5547a5007

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

**EPSS:** 0.000460000 probability, percentile 0.141880000 (date 2026-05-17)

**Problem Types:** CWE-61 | CWE-61 UNIX Symbolic Link (Symlink) Following

Version	Source	Type	Score	Severity	Vector
3.1	f86ef6dc-4d3a-42ad-8f28-e6d5547a5007	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	PostgreSQL	affected 18 18.4 rpm	Not specified
CNA	Na	PostgreSQL	affected 17 17.10 rpm	Not specified
CNA	Na	PostgreSQL	affected 16 16.14 rpm	Not specified
CNA	Na	PostgreSQL	affected 15 15.18 rpm	Not specified
CNA	Na	PostgreSQL	affected 14.23 rpm	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.postgresql.org/support/security/CVE-2026-6475">www.postgresql.org/support/security/CVE-2026-6475</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 Valery Gubanov, XlabAI Team of Tencent Xuanwu Lab, Atuin Automated Vulnerability Discovery Engine, Zhanpeng Liu (pkugenuine(at)gmail(dot)com), Guannan Wang (wgnbuaa(at)gmail(dot)com), and Guancheng Li (lgcpku(at)gmail(dot)com) 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)