Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-6471: Twelve-Year-Old PostgreSQL Flaw Grants Full Server Control

Date of Publication	Admiralty Code	TA Number
September 08, 2026	A1	TA2026262

Summary

First Seen: 2014
Affected Products: PostgreSQL (core server)
Impact: CVE-2026-6471 ("PostGREShell", CVSS 7.2) is a missing-authorization flaw (CWE-862) in PostgreSQL's logical decoding, where a non-superuser REPLICATION role can name an arbitrary library as an output plugin and have the server load and execute it as the postgres OS user, enabling escalation to database superuser and persistent backdoor access. The defect has been latent since version 9.4 (2014) and affects all supported branches before 18.6, 17.11, 16.15, 15.19, and 14.24, patched August 13, 2026. Exploitation requires a REPLICATION credential and wal_level = logical; it is fileless over SMB on Windows but needs file-write access on Linux/macOS. It is not known to be exploited in the wild, though a public proof-of-concept exists. Patch to a fixed release, revoke unnecessary REPLICATION privileges, and restrict replication access to trusted hosts.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-6471	(PostGREShell) PostgreSQL Output Plugin Missing Authorization Vulnerability	PostgreSQL (core server)	✗	✗	✓

Vulnerability Details

#1

CVE-2026-6471 is a high-severity flaw (CVSS 7.2) in PostgreSQL's logical decoding subsystem, arising from missing authorization (CWE-862) in how the server loads output plugins during logical replication. When a replication-capable client creates a logical replication slot, it names the output plugin the server should load; on affected versions that name reaches the library loader without the authorization and path checks applied to the SQL loading path. A role holding only the REPLICATION attribute, not a superuser, can therefore specify an arbitrary filesystem path as the plugin, causing the server to load and execute that shared library within its own backend process.

#2

Because that code runs below the SQL permission layer, it bypasses roles, ACLs, and row-level security entirely. In demonstrated exploitation the loaded library writes to the role catalog to grant itself permanent superuser status and establishes persistence, rewriting host-based authentication for passwordless access, preloading the payload into every new backend, and reapplying superuser if reverted. Two conditions must hold: a REPLICATION-capable credential and wal_level = logical. The route to code execution is platform-dependent: on Windows the plugin name resolves over SMB from an attacker server with nothing written to disk, whereas on Linux and macOS the attacker generally needs file-write access first, making it a second-stage flaw there.

#3

The defect has existed since logical decoding shipped in PostgreSQL 9.4 in 2014, latent for roughly twelve years, and affects every supported branch before the fix. PostgreSQL patched it on August 13, 2026 in releases 18.6, 17.11, 16.15, 15.19, and 14.24; branches 9.4-13 are end-of-life and unpatched. The fix adds a reloadable server parameter that acts as an allow-list of libraries permitted to load as output plugins, defaulting to the built-in plugins only, so third-party output plugins will fail to initialize until explicitly added.

#4

At the time of writing the vulnerability is not known to be exploited in the wild, however, a public proof-of-concept reproducing the full replication-role-to-superuser chain is available, which raises exploitation likelihood. Patch to a fixed release, revoke unnecessary REPLICATION privileges, restrict replication access to known hosts, and rotate replication credentials given the twelve-year exposure window

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-6471	PostgreSQL core server before 18.6, 17.11, 16.15, 15.19, and 14.24	cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:*:*:*	CWE-862

Recommendations

Patch to a Fixed Release Immediately: Upgrade affected instances to PostgreSQL 18.6, 17.11, 16.15, 15.19, or 14.24, or to the equivalent distribution or managed-service package. For package-managed installations the minor upgrade is applied in place and requires only a service restart; patch standby replicas first and schedule the primary restart around replication lag. Where PostgreSQL is consumed as a managed service, confirm the provider has applied the engine patch and verify the instance's effective minor version rather than assuming the latest available version carries the fix.

Prepare for the Post-Patch Plugin Allow-List: The fix introduces an allow-list of permitted output plugins that by default admits only the two plugins shipped with PostgreSQL, so any third-party output plugin will stop loading after the update until it is added to that list and the configuration is reloaded. Before updating, inventory the plugins actually in use by querying the distinct non-null plugin values in the replication-slots view, cross-check the result with data teams, and after updating add each required third-party plugin to the allow-list and reload the configuration, which does not require a restart. When migrating with pg_upgrade from version 17 or later, set the allow-list on the new cluster before running the check step, since the check fails if the list does not permit the old cluster's slot plugins.

Inventory and Reduce the REPLICATION Population: Enumerate every role carrying the REPLICATION attribute and assign each an owner and a purpose; revoke the attribute from any role not actively driving a replica, connector, or backup job, and remember that superuser implies replication capability and warrants the same scrutiny. This inventory is the single most decisive factor in whether the flaw is a theoretical risk or an open door, because it directly determines the population of accounts through which the vulnerability can be reached.

Tighten Replication Access and Network Egress: Scope every replication entry in host-based authentication to the exact source addresses of legitimate consumers, prefer strong password authentication wrapped in TLS, and eliminate broad-CIDR or trust entries. As a compensating control while patching is staged, block outbound SMB and NFS traffic from database servers and disable network-filesystem automounting where it is not required, which closes the fileless Windows and automount-dependent exploitation routes. If no consumer reads logical changes, returning wal_level to replica removes the starting condition entirely at the cost of a restart.

Rotate Replication Credentials and Hunt Retroactively: Treat any replication credential stored in connector configurations, container secrets, or CI variables as potentially exposed over the flaw's twelve-year lifetime, rotate those credentials after patching, and move them into a managed secret store. Given the exposure window, hunt historical telemetry for the database backend process spawning shells, interpreters, or download utilities, for unexpected replication connections and for replication-slot plugin names containing path separators or traversal sequences, and for catalog and configuration changes that grant superuser, loosen authentication, or register new preloaded libraries.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
Execution	T1129: Shared Modules	
	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1556: Modify Authentication Process	

Patch Link

https://www.postgresql.org/support/security/CVE-2026-6471/

References

https://www.postgresql.org/support/security/CVE-2026-6471/

https://github.com/goldendivider/cve-2026-6471-postgres-logical-decoding-dlopen

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 08, 2026 • 05:01 PM

More at www.hivepro.com