SQL Injection în biblioteca ADOdb pentru PHP

Cod CVE	CVE-2025-45337	
Scor	10.0 CRITIC	
CWE	CWE-89 – Neutralizarea necorespunzătoare a elementelor speciale utilizate în comenzile SQL (SQL Injection)	
Descriere	O vulnerabilitate critică a fost identificată în biblioteca *ADOdb* pentru *PHP*, care afectează driverele *PostgreSQL* (***postgres64***, ***postgres7***, ***postgres8***, ***postgres9***). Problema se află în funcția ***pg_insert_id(),*** care nu efectuează neutralizarea corespunzătoare a parametrilor furnizați de utilizator, permițând injectarea de cod *SQL* arbitrar. Aceasta poate fi exploatată atunci când date nesigure (furnizate de utilizator) sunt transmise ca parametru ***$fieldname*** către ***pg_insert_id()*** fără o validare adecvată, ceea ce oferă atacatorului posibilitatea de a executa comenzi *SQL* neautorizate.	
Vectori de Atac și Impact	Vector de atac	Rețea
	Complexitatea atac	Redusă
	Interacțiune utilizator	Nu este necesară
	Privilegii necesare	Niciunul
	Domeniu afectat	Schimbat
Sistemul afectat	ADOdb versiuni până la **5.22.8**	
Componenta afectată	Drivere PostgreSQL (***postgres64, postgres7, postgres8, postgres9***)	
Metode de exploatare	Funcția ***pg_insert_id()*** din biblioteca *ADOdb* pentru *PHP* este utilizată pentru a obține *ID*-ul rezultat în urma unei inserții în *PostgreSQL*. Această funcție permite specificarea opțională a numelui câmpului (***$fieldname***) în care se caută ultimul *ID* inserat. Problema apare când acest parametru nu este corect „scăpat” (escaped), iar valorile transmise provin din surse nesigure (ex. input utilizator), ceea ce duce la injectarea directă de *SQL* în interogare.	
Metode de Detectare	1. Audit manual al codului sursă: • Căutarea apelurilor ***pg_insert_id()*** în fișierele PHP: „ grep -R "pg_insert_id" /var/www/html/ ” • Verificarea valorilor transmise ca ***$fieldname*** pentru a detecta input din surse nesigure (ex***: $_GET, $_POST, $_REQUEST***). 2. Scanare automată: • Utilizarea unor unelte precum *SonarQube, PHPStan* sau *RIPS* pentru detecția funcțiilor sensibile cu parametri nefiltrați. • Integrare cu instrumente de tip *SAST* (Static Application Security Testing). 3. Monitorizare aplicație (Runtime): • Activarea logării tuturor comenzilor *SQL* emise către baza de date *PostgreSQL*. • Detectarea modelelor de query-uri anormale sau neobișnuit de dinamice.	
Exploatare ulterioară	• CVE-2020-13692 – Escaladare a privilegiilor în PostgreSQL • CVE-2021-23214 – SQL Injection în aplicații web care rulează pe PHP și PostgreSQL • CVE-2018-1058 – Scurgere de informații prin abuzarea rolurilor implicite în PostgreSQL	
Metode de remediere	1. Actualizare imediată: • Se recomandă actualizarea la **ADOdb v5.22.9**, care conține patch-ul pentru această vulnerabilitate. 2. Măsuri temporare (dacă actualizarea nu este posibilă):	

	• Validați riguros orice valoare transmisă ca parametru ***$fieldname***. • Utilizați funcția ***pg_escape_identifier()*** pentru a scăpa identificatorii *PostgreSQL*.
Referințe	https://nvd.nist.gov/vuln/detail/CVE-2025-46337 https://github.com/ADOdb/ADOdb/security/advisories/GHSA-8x27-jwjr-8545 https://securityonline.info/critical-sql-injection-vulnerability-found-in-adodb-php-library-cve-2025-46337-cvss-10-0/