BOLETÍN DE ALERTA

Boletín Nro.: 2024-10
Fecha de publicación: 22/02/2024
Tema: Vulnerabilidad crítica de inyección SQL en PostgreSQL

Productos afectados:
-Versiones anteriores a 42.7.2, 42.6.1, 42.5.5, 42.4.4, 42.3.9 y 42.2.8 de pgjdbc.

Descripción:

Se ha reportado una vulnerabilidad crítica en pgjdbc, el controlador JDBC de PostgreSQL, identificada como CVE-2024-1597, con puntuación CVSS de 10.0, la misma permite a un atacante inyectar SQL al utilizar PreferQueryMode=SIMPLE. Aunque este no es el modo predeterminado, en el modo por defecto no existe la vulnerabilidad.
Para explotar la vulnerabilidad, es necesario que un marcador de posición para un valor numérico esté inmediatamente precedido por un signo negativo y que haya un segundo marcador de posición para un valor de cadena después del primero, ambos en la misma línea. Al construir una carga útil de cadena coincidente, el atacante puede inyectar SQL para alterar la consulta, eludiendo las protecciones que las consultas parametrizadas ofrecen contra ataques de inyección SQL.

Impacto:

La vulnerabilidad podría permitir a un actor malicioso realizar inyecciones SQL y alterar consultas, evitando las protecciones de las consultas parametrizadas contra ataques de inyección SQL.

Recomendación:

Se recomienda actualizar pgjdbc a la versión 42.7.2 o posterior desde la página oficial https://www.postgresql.org/download/
Como alternativa, se puede ajustar la configuración y no utilizar la propiedad de esta forma *preferQueryMode=simple*.

Información adicional:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1597
- https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-24rp-q3w6-vc56
- https://www.postgresql.org/about/news/postgresql-jdbc-4272-4261-4255-4244-4239-42228-and-42228jre7-security-update-for-cve-2024-1597-2812/