

¡Publicado PostgreSQL 9.4.2, 9.3.7, 9.2.11, 9.1.16 y 9.0.20!

El Grupo de Desarrollo Global de PostgreSQL ha lanzado una actualización con múltiples funcionalidades nuevas y correcciones de fallos de seguridad, para todas las versiones soportadas de la base de datos PostgreSQL, incluyendo las versiones menores 9.4.2, 9.3.7, 9.2.11, 9.1.16 y 9.0.20. La actualización contiene una corrección crítica para un potencial fallo de corrupción de datos en PostgreSQL 9.3 y 9.4. Los usuarios de estas versiones deberían actualizar sus servidores a la mayor prontitud posible.

Corrección del problema de corrupción de datos

Para los usuarios de PostgreSQL 9.3 ó 9.4, estas actualizaciones solucionan un problema donde la base de datos no protegía frente a "multixact wraparound", lo que podría dar lugar a corrupción o pérdida de datos. Son especialmente vulnerables los usuarios con un volumen elevado de transacciones (1 millón o más por hora) en una base de datos con muchas claves externas (foreign keys). Recomendamos encarecidamente a los usuarios de 9.3 y 9.4 que actualicen sus instalaciones en los próximos días.

Los usuarios de las versiones 9.2 y anteriores no están afectados por este problema.

Actualizaciones de seguridad

Esta actualización soluciona también tres vulnerabilidades de seguridad aparecidas durante los pasados meses. Ninguna de dichas vulnerabilidades está considerada particularmente urgente. A pesar de ello, se recomienda examinarlas para determinar si las instalaciones son vulnerables:

- [CVE-2015-3165](#). Doble "liberación" tras expiración del tiempo de autenticación.
- [CVE-2015-3166](#). Errores no esperados de la librería estándar.
- [CVE-2015-3167](#). pgcrypto tiene múltiples mensajes de error para el descifrado con una clave incorrecta.

Adicionalmente, se recomienda que todos los usuarios que usen autenticación con Kerberos, GSSAPI o SSPI ajusten a 1 el parámetro de configuración `include_realm` en `pg_hba.conf`, lo que será el valor por defecto en siguientes versiones.

Hay disponible más información acerca de estos fallos de seguridad, así como de anteriores, en la Página de Seguridad de PostgreSQL ([PostgreSQL Security Page](#)).

Otras correcciones y mejoras

Una nueva versión de la extensión `citext`, no instalada por defecto, unifica el comportamiento de las funciones no documentadas `regexp_matches()` con la versión ordinaria de texto de las mismas. Esta versión corregida tiene un tipo de retorno diferente de la anterior versión, por lo que los usuarios de `CIText` deberían probar sus aplicaciones antes de actualizar la función mediante el comando "ALTER EXTENSION `citext` UPDATE".

Adicionalmente a lo anterior, se han corregido en esta actualización más de 50 incidencias reportadas. La mayor parte de ellas afectaban a todas las versiones soportadas. Estas correcciones incluyen:

- Mostrar como infinito fechas y timestamps cuando se convierten a json.
- Corregir las funciones json/jsonb populate_record() y to_record().
- Arreglar comprobación incorrecta en restricciones exclusivas postpuestas (deferred exclusion constraints).
- Mejorar la planificación de consultas sobre schemas en formato estrella.
- Corregir tres problemas con operaciones join.
- Asegurar locking correcto en las vistas con protección de seguridad (security barriers).
- Evitar interbloqueo al inicio si max_prepared_transactions es demasiado pequeño.
- Ejecutar fsync() de manera recursiva en el directorio de datos tras una caída.
- Corregir el potencial fallo del lanzador de autovacuum que prevendría su detención.
- Gestionar señales inesperadas en LockBufferForCleanup().
- Arreglar una caída al ejecutar COPY IN sobre una tabla con restricciones "check".
- Evitar esperar para la replicación síncrona en transacciones de sólo lectura.
- Arreglar dos problemas con los índices "hash".
- Evitar pérdida de memoria en el vacuum de un índice GIN.
- Corregir dos problemas en background workers.
- Varios arreglos en la replicación lógica.
- Corregir varios fallos menores en pg_dump y pg_upgrade.

Esta versión incluye también la actualización de tzdata a la versión 2015d, con actualizaciones para Egipto, Mongolia y Palestina, así como cambios históricos en Canadá y Chile.

Próximo el fin de soporte para 9.0

La versión 9.0 dejará de estar soportada (EOL) en septiembre de 2015. Esto implica que esta actualización es posible que sea la última. Los usuarios de PostgreSQL 9.0 deberían comenzar a planificar actualizar a una versión más actual. Puede consultar nuestra [política de versiones y soporte](#) para más información.

Tal y como sucede con las versiones menores, no es necesario hacer un volcado y restauración de la base de datos, ni usar pg_upgrade, para aplicar estas actualizaciones; basta con detener PostgreSQL y actualizar los binarios. Los usuarios de la extensión CIText necesitan ejecutar un comando adicional. Los usuarios que no hayan realizado actualizaciones menores anteriores podrían tener que ejecutar comandos post-actualización; consulte para ello las notas de versiones anteriores.