Boletín de alerta

Boletín Nro.:
Fecha de publicación: 04/03/2026
Tema: Alerta 2026-21 Vulnerabilidad Crítica en pgvector Afecta PostgreSQL
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- pgvector versiones **0.6.0 a 0.8.1**

Implementaciones sobre sistemas Linux/Unix como Debian y Ubuntu que tengan instalada la version vulnerable

Descripción

Se identificó la vulnerabilidad **CVE-2026-3172** (CVSS 8.1 – Alta), relacionada con un desbordamiento de búfer durante la construcción paralela de índices HNSW en pgvector.

Pgvector es una extensión de código abierto para PostgreSQL que permite almacenar, indexar y realizar búsquedas de similitud sobre datos vectoriales (embeddings), siendo ampliamente utilizada en proyectos de inteligencia artificial, búsqueda semántica y sistemas de recomendación.

Esta falla podría permitir que un usuario con acceso a la base de datos acceda a información confidencial de otras tablas o provoque la caída del servidor mediante una denegación de servicio. Aunque su explotación requiere ciertas condiciones técnicas específicas, el riesgo impacta directamente la confidencialidad y la disponibilidad del servicio, por lo que se recomienda actualizar a la versión más reciente disponible.

Es importante señalar que esta extensión no se instala ni habilita por defecto en PostgreSQL. En muchos servicios de bases de datos gestionadas, como Google Cloud SQL, AWS RDS o Azure Database for PostgreSQL, la extensión suele venir preinstalada y solo requiere activación.

Para verificar si pgvector está habilitado, se puede utilizar el comando **\dx** en la consola psql o ejecutar la consulta **SELECT * FROM pg_extension WHERE extname = 'vector';**.

Solución:

Actualizar inmediatamente a la versión más reciente disponible de pgvector.

Información adicional:

https://www.postgresql.org/about/news/pgvector-082-released-3245

https://www.tenable.com/plugins/nessus/300149

https://access.redhat.com/security/cve/cve-2026-3172

https://www.cve.org/CVERecord?id=CVE-2026-3172