DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°188**	**Fecha: 11-08-2023**
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en PostgreSQL		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se han reportado múltiples vulnerabilidades de severidad **MEDIA** de tipo neutralización incorrecta de elementos especiales utilizados en un comando SQL (inyección SQL) y permisos, privilegios y controles de acceso en PostgreSQL. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos de la aplicación.

2. DETALLES:

La vulnerabilidad registrada con el código CVE-2023-39417, de severidad **media** de tipo inyección SQL, existe debido a una desinfección insuficiente de los datos proporcionados por el usuario dentro del script de extensión @substitutions@, que usa @extowner@, @extschema@ o @extschema:...@ dentro de una construcción de comillas. Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación.

Esta vulnerabilidad construye todo o parte de un comando SQL utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar el comando SQL previsto cuando se envía a un componente descendente.

Se ha asignado el siguiente identificador para la vulnerabilidad de severidad baja: CVE-2023-39418.

A. Productos afectados:

- PostgreSQL: 11.0 - 15.3.

3. RECOMENDACIONES:

- Actualizar el paquete afectado con la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.postgresql.org/about/news/postgresql-154-149-1312-1216-1121-and-postgresql-16-beta-3-released-2689/