BOLETÍN DE ALERTA

Boletín Nro.: 2023-47
Fecha de publicación: 28/09/2023
Tema: Vulnerabilidad de ejecución remota de código (*RCE*) en pgAdmin 4

Productos afectados:

- pgAdmin 4, versiones anteriores a 7.7.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a pgAdmin 4, que permitiría a un actor malicioso autenticado realizar ejecución remota de código (*RCE*) en el servidor afectado.

La vulnerabilidad identificada como CVE-2023-5002, de severidad "Alta" y con puntuación asignada de 8.8. La vulnerabilidad se produce cuando el servidor *HTTP API* de pgAdmin valida la ruta que el usuario selecciona para utilizar utilidades externas de PostgreSQL, como *pg_dump* y *pg_restore*. Esto permitiría a un actor malicioso autenticado a través de la *API* del servidor, realizar ejecución de comandos arbitrarios.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un actor malicioso autenticado realizar ejecución de código arbitrario en el servidor afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través del siguiente enlace:

- https://www.pgadmin.org/download/

Información adicional:

- https://securityonline.info/cve-2023-5002-pgadmin-remote-code-execution-vulnerability/?expand_article=1#google_vignette
- https://nvd.nist.gov/vuln/detail/CVE-2023-5002
- https://www.postgresql.org/about/news/pgadmin-4-v77-released-2723/
- https://www.pgadmin.org/download/