

Alerta ID:	113
Fecha del reporte:	22/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Múltiples vulnerabilidades críticas en pgAdmin 4 podrían permitir secuestro de sesiones, acceso no autorizado y compromiso de plataformas de administración de bases de datos PostgreSQL
Herramienta de detección	N/A
Activo involucrado:	pgAdmin 4; servidores PostgreSQL; plataformas de administración de bases de datos; servidores Linux y Windows; sistemas de información clínicos; plataformas de historia clínica electrónica; aplicaciones administrativas; servicios de interoperabilidad; ambientes de desarrollo, pruebas y producción que utilicen pgAdmin 4.
Tipo de alerta:	Alerta
Nivel de riesgo:	Critico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la publicación de múltiples vulnerabilidades de seguridad identificadas en pgAdmin 4, herramienta ampliamente utilizada para la administración y gestión de bases de datos PostgreSQL.

Las vulnerabilidades corregidas por los desarrolladores del proyecto afectan componentes utilizados para la autenticación, gestión de sesiones, procesamiento de solicitudes web y manejo de contenido presentado a los usuarios dentro de la interfaz administrativa de la plataforma.



El propósito de esta alerta es que las entidades evalúen el impacto potencial que estas vulnerabilidades podrían generar sobre:

- servidores PostgreSQL institucionales;
- plataformas de administración de bases de datos;
- sistemas de historia clínica electrónica;
- aplicaciones clínicas y administrativas;
- plataformas de interoperabilidad en salud;
- servicios de analítica y procesamiento de datos;
- repositorios de información sensible;
- ambientes de desarrollo y producción;
- servicios accesibles mediante interfaces web;
- y activos críticos administrados mediante pgAdmin 4.

Asimismo, se busca generar conciencia sobre los riesgos asociados a la exposición de consolas administrativas accesibles desde Internet, configuraciones inseguras de autenticación y explotación de vulnerabilidades web que podrían ser utilizadas para comprometer activos críticos de información.

En el contexto del sector salud, este escenario representa un riesgo significativo debido a la dependencia de bases de datos PostgreSQL para soportar procesos clínicos, administrativos, financieros y operativos, así como para almacenar información personal, datos sensibles de pacientes e información relacionada con la prestación de servicios de salud.

Descripción:



Los desarrolladores de pgAdmin publicaron actualizaciones de seguridad destinadas a corregir múltiples vulnerabilidades identificadas en la plataforma de administración PostgreSQL pgAdmin 4. Las fallas afectan diversos componentes de la aplicación y podrían ser aprovechadas por actores maliciosos para ejecutar ataques orientados al compromiso de



cuentas administrativas, secuestro de sesiones, ejecución de acciones no autorizadas y acceso indebido a información sensible.

De acuerdo con la información técnica divulgada por el fabricante, las vulnerabilidades corregidas incluyen debilidades relacionadas con mecanismos de autenticación, validación insuficiente de entradas, controles de acceso, protección de sesiones y componentes susceptibles a ataques de Cross-Site Scripting (XSS).

La explotación exitosa de estas vulnerabilidades podría permitir que un atacante obtenga acceso no autorizado a funciones administrativas de la plataforma, comprometa sesiones activas de usuarios legítimos o ejecute acciones utilizando los privilegios de administradores autenticados.

Uno de los aspectos más relevantes de este escenario corresponde a que pgAdmin constituye una de las herramientas más utilizadas para la administración de bases de datos PostgreSQL en entornos corporativos, gubernamentales, académicos y de salud.

Las plataformas PostgreSQL administradas mediante pgAdmin suelen almacenar información crítica relacionada con procesos institucionales, registros operativos, datos financieros, información contractual, registros clínicos, datos personales y otra información estratégica para la organización.

Las vulnerabilidades identificadas podrían ser aprovechadas mediante la interacción de usuarios legítimos con contenido especialmente preparado por los atacantes o mediante el acceso a instancias vulnerables expuestas a redes internas o externas.

Dependiendo de la configuración implementada por cada organización, un atacante podría obtener acceso a funcionalidades administrativas de la plataforma, visualizar información sensible, alterar configuraciones, crear cuentas no autorizadas, modificar estructuras de bases de datos o ejecutar acciones que afecten la integridad de la información almacenada.



La exposición de interfaces administrativas de bases de datos representa un riesgo significativo debido a que estas plataformas concentran privilegios elevados sobre activos críticos de información. En muchos entornos, los administradores utilizan pgAdmin para gestionar múltiples servidores PostgreSQL desde una única consola centralizada, incrementando el impacto potencial de un compromiso exitoso.

En el contexto del sector salud, la explotación de estas vulnerabilidades podría afectar directamente plataformas utilizadas para soportar historias clínicas electrónicas, sistemas de laboratorio, aplicaciones de imágenes diagnósticas, servicios de interoperabilidad, sistemas de referencia y contrarreferencia, plataformas administrativas hospitalarias y otras aplicaciones que dependen de bases de datos PostgreSQL para su funcionamiento.

Las organizaciones que utilicen versiones vulnerables de pgAdmin deben considerar esta situación como una amenaza prioritaria debido al potencial acceso a información altamente sensible y a la posibilidad de que los atacantes utilicen la plataforma comprometida como punto de entrada hacia otros activos tecnológicos de la organización.

En consecuencia, resulta fundamental que las entidades identifiquen de manera inmediata las instancias de pgAdmin desplegadas en sus infraestructuras, verifiquen las versiones instaladas y adopten las medidas de actualización y mitigación recomendadas por el fabricante.

Consecuencias de la explotación

La explotación exitosa de las vulnerabilidades identificadas en pgAdmin 4 podría generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de la información institucional.

Uno de los principales riesgos asociados corresponde al acceso no autorizado a plataformas administrativas utilizadas para gestionar bases de datos PostgreSQL que soportan procesos críticos de la organización.



En escenarios vulnerables, un atacante podría aprovechar estas debilidades para:

- secuestrar sesiones activas de administradores;
- ejecutar acciones administrativas no autorizadas;
- acceder a información sensible almacenada en bases de datos;
- modificar configuraciones críticas;
- crear cuentas con privilegios elevados;
- comprometer credenciales institucionales;
- y obtener acceso persistente a la infraestructura tecnológica.

Uno de los impactos más relevantes corresponde a la posible exposición de información sensible almacenada dentro de las bases de datos administradas mediante pgAdmin.

La explotación exitosa podría permitir el acceso no autorizado a:

- información clínica de pacientes;
- datos personales protegidos;
- registros administrativos;
- información financiera;
- información contractual;
- credenciales de acceso;
- configuraciones institucionales;
- y documentación interna de la organización.

La pérdida de confidencialidad de estos activos podría generar consecuencias regulatorias, legales, operacionales y reputacionales para las entidades afectadas.

Otro riesgo significativo corresponde a la alteración no autorizada de información almacenada en las bases de datos institucionales.

Dependiendo del alcance obtenido por el atacante, podrían ejecutarse acciones relacionadas con:



- modificación de registros clínicos;
- eliminación de información;
- alteración de configuraciones de aplicaciones;
- creación de usuarios privilegiados;
- manipulación de estructuras de bases de datos;
- modificación de controles de acceso;
- y afectación de procesos críticos soportados por PostgreSQL.

La explotación también podría facilitar movimientos laterales dentro de la infraestructura institucional.

Una vez comprometida la consola administrativa, los atacantes podrían intentar identificar activos adicionales conectados a la red corporativa.

Las actividades posteriores podrían incluir:

- reconocimiento interno de la infraestructura;
- identificación de servidores críticos;
- descubrimiento de servicios corporativos;
- enumeración de usuarios privilegiados;
- búsqueda de credenciales adicionales;
- identificación de recursos compartidos;
- y acceso progresivo a sistemas de mayor valor para la organización.

En el contexto del sector salud, los riesgos adquieren una relevancia especial debido a la naturaleza sensible de la información procesada por las entidades.

La explotación exitosa podría afectar directamente plataformas utilizadas para:

- gestión de historias clínicas electrónicas;
- sistemas de laboratorio clínico;
- plataformas diagnósticas;



- servicios de telemedicina;
- sistemas administrativos hospitalarios;
- plataformas de interoperabilidad;
- servicios de facturación;
- y repositorios de información clínica protegida.

La indisponibilidad o alteración de estos servicios podría afectar directamente la continuidad operacional y la prestación de servicios de salud.

Modo de explotación del ataque

Fase 1 – Identificación de objetivos potenciales

El proceso de explotación inicia cuando los actores de amenaza identifican organizaciones que utilizan pgAdmin 4 para la administración de entornos PostgreSQL. Debido a que esta herramienta es ampliamente utilizada en entornos empresariales y gubernamentales, los atacantes suelen realizar actividades de reconocimiento orientadas a identificar instancias accesibles desde Internet o disponibles dentro de redes corporativas comprometidas previamente.

Durante esta etapa, los atacantes buscan determinar qué organizaciones utilizan PostgreSQL como plataforma de gestión de bases de datos y cuáles emplean pgAdmin como herramienta de administración centralizada. Esta información puede obtenerse mediante técnicas de reconocimiento abierto (OSINT), análisis de infraestructura expuesta, motores de búsqueda especializados, escaneo de servicios web y recopilación de información pública relacionada con la organización objetivo.

Durante esta fase, los atacantes pueden identificar:

- organizaciones que utilizan PostgreSQL;
- consolas administrativas expuestas a Internet;
- servicios accesibles mediante interfaces web;



- entidades del sector salud;
- ambientes de desarrollo vulnerables;
- usuarios con privilegios administrativos;
- y versiones potencialmente vulnerables de pgAdmin.

El objetivo principal consiste en identificar plataformas susceptibles de explotación que permitan obtener acceso a información sensible o comprometer sistemas de mayor valor para la organización.

Fase 2 – Reconocimiento y análisis de la plataforma

Una vez identificado el objetivo, los actores de amenaza realizan actividades de reconocimiento más detalladas orientadas a comprender la arquitectura de la plataforma y los mecanismos de seguridad implementados.

Durante esta etapa, los atacantes buscan identificar la versión exacta de pgAdmin desplegada, los métodos de autenticación configurados, las funcionalidades habilitadas y la exposición de componentes administrativos que puedan ser aprovechados durante fases posteriores del ataque.

Dependiendo del escenario, también pueden analizar la estructura de la aplicación web, identificar formularios vulnerables, mecanismos de gestión de sesiones, componentes susceptibles a ataques XSS y funcionalidades administrativas accesibles para usuarios autenticados.

Las actividades realizadas durante esta fase pueden incluir:

- identificación de versiones instaladas;
- enumeración de funcionalidades disponibles;
- análisis de mecanismos de autenticación;
- identificación de usuarios administrativos;



- evaluación de controles de acceso;
- reconocimiento de servidores asociados;
- y análisis de posibles vectores de explotación.

El objetivo consiste en determinar la mejor estrategia para comprometer la plataforma con el menor nivel posible de interacción y exposición para el atacante.

Fase 3 – Preparación del vector de ataque

Posteriormente, los actores de amenaza preparan los recursos necesarios para ejecutar la explotación de las vulnerabilidades identificadas.

Dependiendo de la vulnerabilidad específica que pretenda explotarse, los atacantes pueden desarrollar código malicioso, preparar sitios web especialmente diseñados, generar enlaces manipulados o crear cargas útiles destinadas a interactuar con componentes vulnerables de la aplicación.

En escenarios relacionados con vulnerabilidades de Cross-Site Scripting (XSS), los atacantes pueden desarrollar scripts capaces de ejecutarse dentro del contexto de la sesión de usuarios legítimos. Estas capacidades pueden permitir el robo de cookies de autenticación, secuestro de sesiones activas o ejecución de acciones administrativas utilizando los privilegios de la víctima. Durante esta fase podrían desarrollarse actividades relacionadas con:

- preparación de cargas maliciosas;
- desarrollo de scripts de explotación;
- generación de enlaces manipulados;
- preparación de campañas de phishing;
- configuración de infraestructura de comando y control;
- creación de sitios web controlados por atacantes;
- y preparación de mecanismos de persistencia.



El objetivo consiste en disponer de una infraestructura capaz de explotar la vulnerabilidad una vez que la víctima interactúe con el contenido preparado por el atacante.

Fase 4 – Explotación de la vulnerabilidad

Cuando la víctima accede al contenido malicioso o interactúa con la funcionalidad vulnerable, se produce la explotación efectiva de la vulnerabilidad identificada en pgAdmin.

Dependiendo de la falla específica aprovechada, el atacante podría ejecutar código dentro del contexto de la sesión del usuario afectado, manipular solicitudes legítimas enviadas por el navegador, acceder a funcionalidades restringidas o evadir determinados mecanismos de autenticación y control de acceso.

La explotación puede producirse sin requerir interacción adicional del usuario una vez activada la vulnerabilidad, especialmente en escenarios donde se aprovechan fallas relacionadas con la gestión de sesiones o procesamiento de contenido web.

Las actividades realizadas durante esta fase pueden orientarse a:

- secuestrar sesiones activas;
- ejecutar código malicioso en navegadores;
- manipular solicitudes administrativas;
- acceder a funciones privilegiadas;
- comprometer credenciales;
- evadir controles de autenticación;
- y obtener acceso inicial a la plataforma.

El objetivo consiste en lograr la ejecución de acciones controladas por el atacante utilizando los privilegios asociados a la sesión comprometida.



Fase 5 – Obtención de acceso privilegiado

Una vez obtenida una posición inicial dentro de la plataforma, los atacantes buscan ampliar el alcance del compromiso y obtener mayores niveles de acceso sobre el entorno administrativo. En muchos escenarios, las consolas pgAdmin administran múltiples servidores PostgreSQL desde una única interfaz. Como consecuencia, el compromiso de una cuenta privilegiada puede proporcionar acceso a numerosos activos de información distribuidos dentro de la organización. Dependiendo de los privilegios disponibles, los atacantes podrían realizar actividades orientadas a:

- crear cuentas administrativas;
- modificar configuraciones de seguridad;
- acceder a nuevas bases de datos;
- extraer credenciales almacenadas;
- alterar permisos existentes;
- establecer mecanismos de persistencia;
- y ampliar el alcance del compromiso.

El objetivo consiste en consolidar el acceso obtenido y garantizar la continuidad de las actividades maliciosas dentro del entorno comprometido.

Fase 6 – Acceso y recopilación de información sensible

Posteriormente, los actores de amenaza realizan actividades destinadas a identificar, recopilar y extraer información de valor almacenada dentro de las bases de datos administradas por la plataforma.

Debido a que PostgreSQL suele soportar aplicaciones críticas de negocio, la información disponible puede incluir datos personales, información clínica, registros administrativos, información financiera y otros activos estratégicos para la organización.



La información objetivo puede incluir:

- historias clínicas electrónicas;
- datos personales de pacientes;
- credenciales institucionales;
- registros administrativos;
- información financiera;
- configuraciones de aplicaciones;
- documentación interna;
- y datos relacionados con la operación institucional.

La información obtenida puede ser utilizada para actividades de fraude, espionaje, extorsión, venta de información o preparación de ataques posteriores.

Fase 7 – Movimiento lateral y expansión del compromiso

Finalmente, una vez comprometida la plataforma administrativa, los atacantes pueden utilizar el acceso obtenido para extender el alcance del incidente hacia otros activos tecnológicos de la organización.

Las credenciales obtenidas, las conexiones configuradas dentro de pgAdmin y la visibilidad sobre la infraestructura pueden facilitar actividades de movimiento lateral orientadas al compromiso de servidores adicionales.

Las actividades observadas habitualmente incluyen:

- reconocimiento interno de la infraestructura;
- identificación de servidores críticos;
- descubrimiento de nuevos servicios;
- robo de credenciales adicionales;
- acceso a sistemas conectados;
- despliegue de malware;



- exfiltración de información;
- y establecimiento de mecanismos permanentes de acceso.

La capacidad de movimiento lateral incrementa significativamente el impacto potencial del incidente al permitir que los atacantes extiendan el compromiso más allá de la plataforma inicialmente afectada y comprometan activos críticos adicionales dentro de la organización.

Vulnerabilidades asociadas

Cross-Site Scripting (XSS)

- **Descripción:** Una de las vulnerabilidades corregidas en pgAdmin 4 corresponde a una falla de tipo Cross-Site Scripting (XSS), la cual podría permitir que un atacante inyecte y ejecute código JavaScript malicioso dentro del navegador de usuarios autenticados.

Este tipo de vulnerabilidades se presenta cuando la aplicación no valida adecuadamente determinados contenidos antes de procesarlos o presentarlos al usuario. Como resultado, un atacante podría lograr que código malicioso se ejecute dentro de una sesión legítima de pgAdmin, aprovechando los privilegios asociados al usuario afectado.

- **Impacto:** La explotación exitosa de esta vulnerabilidad podría permitir el secuestro de sesiones activas, el robo de cookies de autenticación y la ejecución de acciones administrativas no autorizadas dentro de la plataforma. Asimismo, un atacante podría acceder a información sensible visualizada por el usuario comprometido y utilizar sus privilegios para modificar configuraciones o interactuar con servidores PostgreSQL administrados mediante pgAdmin.

En entornos del sector salud, esta situación podría facilitar el acceso no autorizado a información clínica, administrativa y operativa almacenada en bases de datos institucionales.



Debilidades en la autenticación y control de acceso

- **Descripción:** Las actualizaciones de seguridad también corrigen vulnerabilidades relacionadas con mecanismos de autenticación y control de acceso implementados dentro de pgAdmin. Estas debilidades podrían permitir que usuarios no autorizados accedan a determinadas funcionalidades o interactúen con recursos protegidos de manera indebida.

Dependiendo de la configuración afectada y de las condiciones de explotación, un atacante podría eludir determinadas restricciones de seguridad y ejecutar acciones utilizando privilegios superiores a los que le corresponden.

- **Impacto:** La explotación de estas vulnerabilidades podría facilitar el acceso no autorizado a funcionalidades administrativas, la modificación de configuraciones críticas y la visualización de información restringida. Un atacante que logre explotar estas debilidades podría ampliar progresivamente el alcance del compromiso y afectar activos adicionales dentro de la infraestructura tecnológica.

En organizaciones del sector salud, el acceso indebido a plataformas administrativas podría comprometer sistemas que soportan procesos clínicos, operativos y administrativos críticos.

Gestión insegura de sesiones

- **Descripción:** Las vulnerabilidades identificadas incluyen fallas relacionadas con la gestión de sesiones utilizadas para mantener autenticados a los usuarios dentro de la plataforma. Estas debilidades pueden afectar los mecanismos encargados de validar la identidad de los usuarios durante sus actividades administrativas.



Cuando los controles de gestión de sesiones no son implementados adecuadamente, los atacantes pueden intentar reutilizar identificadores válidos o aprovechar sesiones activas para obtener acceso a recursos protegidos.

- **Impacto:** La explotación exitosa podría permitir el secuestro de sesiones administrativas y la ejecución de acciones utilizando la identidad de usuarios legítimos. Como consecuencia, un atacante podría acceder a información sensible, modificar configuraciones de la plataforma o interactuar con bases de datos institucionales sin necesidad de conocer credenciales válidas.

Este escenario representa un riesgo significativo para organizaciones que administran información sensible mediante PostgreSQL, especialmente en entornos relacionados con la prestación de servicios de salud.

Validación insuficiente de entradas y procesamiento de contenido web

- **Descripción:** Las actualizaciones también corrigen debilidades asociadas a la validación insuficiente de datos procesados por la aplicación. Este tipo de vulnerabilidades puede originarse cuando determinados parámetros o solicitudes no son evaluados adecuadamente antes de ser utilizados por los componentes internos de la plataforma.

La falta de controles apropiados puede facilitar la manipulación del comportamiento esperado de la aplicación y abrir oportunidades para ataques orientados al acceso no autorizado o a la alteración de funcionalidades administrativas.

- **Impacto:** La explotación de estas vulnerabilidades podría permitir la manipulación de solicitudes legítimas, la alteración de configuraciones y el acceso a información que debería permanecer protegida. Adicionalmente, estas debilidades podrían ser utilizadas como punto de partida para ataques más complejos orientados al compromiso de servidores PostgreSQL o de otros activos conectados a la plataforma.



En el sector salud, este escenario podría incrementar la superficie de ataque sobre sistemas que almacenan información clínica, financiera y administrativa de carácter sensible.

Recomendaciones

Considerando la criticidad de las vulnerabilidades identificadas en pgAdmin 4 y el impacto potencial que su explotación podría generar sobre plataformas de administración de bases de datos PostgreSQL, se recomienda a las organizaciones realizar una evaluación inmediata de los activos afectados e implementar las medidas necesarias para reducir la superficie de exposición existente.

Las entidades del sector salud deben prestar especial atención a este tipo de plataformas debido a que frecuentemente administran bases de datos que almacenan información clínica, datos personales, registros financieros y otros activos críticos para la operación institucional. Un compromiso exitoso de una consola administrativa puede facilitar el acceso a múltiples servidores PostgreSQL y aumentar significativamente el alcance de un incidente de seguridad.

Asimismo, se recomienda fortalecer los controles de acceso, monitoreo y gestión de vulnerabilidades asociados a estas plataformas, con el fin de reducir las posibilidades de explotación y detectar oportunamente actividades sospechosas que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Actualización y gestión de vulnerabilidades

La principal medida de mitigación consiste en actualizar todas las instancias de pgAdmin 4 a las versiones corregidas por el fabricante. Las organizaciones deben verificar no solamente los entornos de producción, sino también los ambientes de desarrollo, pruebas y contingencia, ya que estos suelen convertirse en objetivos atractivos para los atacantes debido a controles de seguridad menos estrictos.



Se recomienda establecer procedimientos formales para la gestión de vulnerabilidades que permitan identificar oportunamente nuevas actualizaciones de seguridad y evaluar su impacto sobre los activos institucionales. Asimismo, resulta conveniente realizar análisis periódicos de vulnerabilidades y mantener inventarios actualizados de las plataformas PostgreSQL y herramientas asociadas.

Protección de accesos administrativos

Las plataformas de administración de bases de datos constituyen activos de alto valor para los actores maliciosos debido a los privilegios elevados que normalmente poseen. Por esta razón, se recomienda restringir el acceso únicamente al personal autorizado y aplicar el principio de mínimo privilegio sobre todas las cuentas administrativas.

Las organizaciones deben implementar mecanismos de autenticación multifactor para reducir el riesgo asociado al robo o compromiso de credenciales. Adicionalmente, se recomienda revisar periódicamente los privilegios asignados a usuarios administrativos, eliminar cuentas obsoletas y verificar que no existan credenciales compartidas entre diferentes funcionarios o contratistas.

Seguridad de la infraestructura

Las instancias de pgAdmin no deberían encontrarse expuestas directamente a Internet salvo que exista una necesidad operacional debidamente justificada y acompañada de controles de seguridad adicionales. Siempre que sea posible, se recomienda restringir el acceso mediante VPN institucionales, redes privadas, listas de control de acceso o mecanismos de acceso remoto seguro.

También resulta recomendable implementar esquemas de segmentación de red que permitan aislar los servidores de administración de bases de datos de otros segmentos de la infraestructura tecnológica. Esta medida contribuye a limitar los movimientos laterales en caso de que un atacante logre comprometer alguno de los sistemas expuestos.



Monitoreo y detección

Las organizaciones deben fortalecer las capacidades de monitoreo sobre las actividades realizadas en pgAdmin y PostgreSQL con el fin de identificar comportamientos anómalos o indicios de explotación. Es recomendable revisar periódicamente los registros de auditoría y establecer alertas para detectar actividades administrativas inusuales.

Entre los eventos que deberían generar especial atención se encuentran los intentos reiterados de autenticación fallida, accesos desde ubicaciones inusuales, creación de nuevas cuentas administrativas, modificaciones de configuraciones críticas, cambios en privilegios de usuarios y actividades realizadas fuera de los horarios habituales de operación.

Cuando sea posible, estos eventos deberían integrarse a plataformas SIEM institucionales para facilitar la correlación de eventos y mejorar las capacidades de detección temprana.

Protección de la información y continuidad operativa

Las entidades deben verificar periódicamente la integridad de las bases de datos administradas mediante pgAdmin y asegurar la existencia de mecanismos adecuados de respaldo y recuperación. Las copias de seguridad deben mantenerse actualizadas, protegidas frente a modificaciones no autorizadas y sometidas a pruebas periódicas de restauración.

Adicionalmente, se recomienda revisar los procedimientos de recuperación ante incidentes relacionados con bases de datos y validar que los tiempos de recuperación definidos sean compatibles con las necesidades operacionales de la organización. En el sector salud, la disponibilidad de la información clínica puede resultar crítica para la continuidad de la atención de los pacientes.



Gestión de credenciales y sesiones

Debido a que algunas de las vulnerabilidades corregidas pueden afectar mecanismos de autenticación y gestión de sesiones, se recomienda reforzar las prácticas relacionadas con la protección de credenciales administrativas. Las contraseñas deben cumplir requisitos robustos de complejidad, longitud y renovación periódica.

Asimismo, las organizaciones deberían revisar los tiempos de expiración de sesiones, implementar mecanismos automáticos de cierre por inactividad y verificar que las credenciales utilizadas para la conexión a servidores PostgreSQL se encuentren adecuadamente protegidas y almacenadas.

Respuesta a incidentes

Las áreas de tecnología y seguridad de la información deben revisar los procedimientos de respuesta a incidentes relacionados con bases de datos y plataformas administrativas para garantizar una reacción oportuna ante posibles intentos de explotación.

Ante cualquier evidencia de actividad sospechosa, se recomienda realizar una revisión detallada de registros, validar la integridad de las configuraciones existentes, identificar posibles accesos no autorizados y evaluar el impacto potencial sobre la información institucional. De igual manera, resulta importante coordinar oportunamente las actividades de contención, erradicación y recuperación para minimizar las afectaciones sobre la operación.

La implementación de estas medidas permitirá reducir significativamente la probabilidad de explotación de las vulnerabilidades identificadas y fortalecer la protección de las plataformas PostgreSQL que soportan servicios críticos dentro de las organizaciones del sector salud.



Conclusiones



Las vulnerabilidades recientemente corregidas en pgAdmin 4 representan una amenaza significativa para las organizaciones que utilizan PostgreSQL como plataforma para la gestión y almacenamiento de información crítica. La combinación de fallas asociadas a mecanismos de autenticación, gestión de sesiones, validación de entradas y vulnerabilidades de tipo Cross-Site Scripting (XSS) puede facilitar escenarios de acceso no autorizado, secuestro de sesiones y compromiso de plataformas administrativas que poseen privilegios elevados sobre activos institucionales.

La explotación exitosa de estas vulnerabilidades podría permitir a los actores maliciosos obtener acceso a información sensible, alterar configuraciones críticas, comprometer credenciales administrativas y ampliar progresivamente el alcance de un incidente hacia otros componentes de la infraestructura tecnológica. Debido a que pgAdmin es utilizado para administrar múltiples servidores PostgreSQL desde una única interfaz, un compromiso exitoso podría tener consecuencias que trasciendan el sistema inicialmente afectado y generar impactos relevantes sobre la operación institucional.

En el sector salud, el riesgo asociado adquiere una relevancia especial debido a la naturaleza de la información procesada y almacenada en las bases de datos institucionales. Historias clínicas electrónicas, datos personales de pacientes, registros administrativos, información financiera y otros activos estratégicos podrían verse expuestos o afectados como consecuencia de la explotación de estas vulnerabilidades, generando implicaciones operativas, regulatorias, legales y reputacionales para las entidades comprometidas.

La publicación de las actualizaciones de seguridad por parte del fabricante proporciona a las organizaciones la oportunidad de reducir significativamente el riesgo asociado a estas vulnerabilidades. Sin embargo, la efectividad de estas medidas dependerá de la capacidad de las entidades para identificar oportunamente los sistemas afectados, aplicar las correcciones disponibles y fortalecer los controles de seguridad relacionados con la administración de bases de datos y la gestión de accesos privilegiados.



En consecuencia, se recomienda a las organizaciones del sector salud priorizar la actualización de las instancias de pgAdmin 4, reforzar los mecanismos de monitoreo y control de acceso, y mantener una vigilancia continua sobre las actividades administrativas realizadas dentro de estas plataformas. La adopción oportuna de estas medidas contribuirá a fortalecer la postura de ciberseguridad institucional y a reducir la probabilidad de materialización de incidentes que puedan afectar la confidencialidad, integridad y disponibilidad de la información crítica para la prestación de servicios de salud.

Fuentes:



- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk>
- <https://www.postgresql.org/about/news/pgadmin-4-v916-released-3324/>
- https://www.pgadmin.org/docs/pgadmin4/9.16/release_notes_9_16.html
- <https://www.pgadmin.org/>
- <https://securityonline.info/pgadmin-4-vulnerabilities/>
- <https://www.postgresql.org/about/news/>
- <https://www.cve.org/>
- <https://nvd.nist.gov/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

