Historia de cliente de Akamai

Una empresa de deportes y medios de comunicación descubre los riesgos de las API ocultas

Al crear un inventario de API completo, esta empresa descubrió errores de configuración que abrían las puertas a los ataques de API

Creación de un inventario preciso

Detección de controles omitidos

Inyección SQL detectada

Las plataformas y aplicaciones digitales están revolucionando el sector de los deportes y los medios de comunicación gracias a la potencia de las API. Estos avances tecnológicos están transformando la forma en la que se organizan, se promocionan y se viven los eventos en directo, lo que genera nuevas oportunidades para los artistas, los organizadores de eventos y el público.

Las API pueden compartir de manera fluida información y actualizaciones de los eventos, así como los enlaces a las entradas, a través de varios canales de redes sociales, lo que aumenta la visibilidad y fomenta la venta de entradas. Además, las API están revolucionando la experiencia in situ de los eventos en directo. La integración con aplicaciones móviles y dispositivos portátiles hace posible el uso de funciones interactivas, como programaciones personalizadas, mapas interactivos y notificaciones en tiempo real.

Sin embargo, dada la naturaleza confidencial de las transacciones y los datos involucrados en el sector de los deportes y los medios de comunicación, es esencial priorizar la seguridad de API. Los controles de seguridad de las API desempeñan un papel fundamental a la hora de garantizar la integridad, la confidencialidad y la disponibilidad de los datos. Por esa razón, esta organización de deportes y medios de comunicación de renombre mundial se puso en contacto con Noname Security (ahora una empresa de Akamai).

Adopción de medidas de seguridad de API

El cliente era muy consciente de la necesidad de implementar medidas de seguridad de API, pero no tenía claro por dónde debía empezar y qué áreas debían priorizarse. Tradicionalmente, se había centrado en la seguridad de las aplicaciones y creía que sus herramientas, como las puertas de enlace de API y los firewalls de aplicaciones web, eran

Sports and Media Company

Ubicación

Estados Unidos

Sector

Medios de comunicación y entretenimiento

Solución

Akamai API Security

Akamai

suficiente para proteger las API. No obstante, aunque herramientas como estas pueden garantizar ciertas protecciones básicas, no están diseñadas para proporcionar el grado de visibilidad, protección en tiempo real y pruebas continuas que pueden ofrecer las soluciones de seguridad de API especializadas. Por otro lado, con su infraestructura, no era posible implementar muchas de estas estrategias de seguridad especializadas. Por ejemplo, dos de los aspectos clave de la seguridad de API son la autenticación y la autorización. Contar con mecanismos de autenticación adecuados en las API garantiza que solo los usuarios o sistemas autorizados puedan acceder a ellas.

Detección de vulnerabilidades

El equipo de Akamai API Security utilizó los módulos de gestión de la situación y protección del tiempo de ejecución para comprender la estrategia de seguridad de API del cliente. Una vez que contamos con un inventario preciso de las API en el entorno del cliente, pudimos detectar vulnerabilidades de seguridad y errores de configuración.

Lo primero que descubrimos fue que el cliente había sido víctima de un ataque de inyección de lenguaje de consulta estructurado (SQLi). SQLi es un tipo de vulnerabilidad de seguridad que se produce cuando un atacante puede manipular los parámetros de entrada de una solicitud de API para ejecutar comandos SQL no autorizados. Las consecuencias de un ataque SQLi pueden ser nefastas. Los atacantes pueden obtener acceso no autorizado a datos confidenciales, modificar o eliminar datos, o incluso ejecutar comandos arbitrarios en el servidor de bases de datos subyacente.

Lo segundo que detectamos fue que el cliente no contaba con medidas de autenticación. Sin un método de autenticación fiable, cualquier persona puede acceder a los terminales de API y extraer, eliminar o modificar datos confidenciales, lo que conllevaría problemas de integridad de datos y una posible pérdida de información esencial. Esto puede dar lugar a filtraciones de datos, una divulgación de información no autorizada o incluso comprometer al sistema por completo.

Perspectivas de futuro

Ahora que el cliente tiene un firme control sobre sus API en fase de producción, ha estado investigando cómo abordar las vulnerabilidades antes de esa fase. Para ayudar a las organizaciones a encontrar y corregir estas vulnerabilidades, Akamai API Security incluye Active Testing, una solución de pruebas de seguridad de API diseñada específicamente y que es capaz de comprender la lógica empresarial de una organización y proporcionar una cobertura completa de las vulnerabilidades específicas de sus API. Con Active Testing, cualquier organización podrá realizar de forma temprana y frecuente, así como integrar, las pruebas de seguridad de API en todas las fases del desarrollo.

 | Publicado en septiembre de 2024