História do cliente da Akamai

Empresa de esportes e mídia revela riscos ocultos às APIs

Criar um inventário de APIs completo e descobrir configurações incorretas que abrem portas para ataques de API

Criou um inventário preciso

Detectou ausência de controles

Descobriu injeção de SQL

Plataformas e aplicativos digitais estão revolucionando o setor de esportes e mídia com o poder das APIs. Esses avanços tecnológicos estão transformando a forma como os eventos ao vivo são organizados, promovidos e vivenciados, criando oportunidades para artistas, organizadores de eventos e públicos.

As APIs podem compartilhar facilmente informações, atualizações e links de ingressos para eventos em vários canais de mídia social, aumentando a visibilidade e a venda de ingressos. Além disso, as APIs estão transformando a experiência no local em eventos ao vivo. A integração com aplicativos móveis e dispositivos vestíveis habilita recursos interativos, como programações personalizadas, mapas interativos e notificações em tempo real.

No entanto, é importante notar que a natureza confidencial dos dados e transações envolvidas no setor de esportes e mídia torna imperativo priorizar a segurança de APIs. Os controles de segurança de APIs desempenham um papel fundamental na garantia da integridade, confidencialidade e disponibilidade de dados, e é por isso que esta organização de esportes e mídia mundialmente renomada recorreu à Noname Security (agora uma empresa Akamai).

Adoção da segurança de APIs

O cliente estava bem ciente da necessidade de segurança de APIs, mas não tinha muita certeza de onde deveria começar e quais áreas deviam ser priorizadas. Tradicionalmente, ele estava focado principalmente na segurança de aplicativos e pensava que suas ferramentas existentes, como gateways de API e firewalls de aplicativos da Web, seriam suficientes para proteger APIs. No entanto, embora ferramentas como essas possam oferecer certas proteções básicas, elas não foram

Sports and Media Company

Localização

Estados Unidos

Setor

Mídia e entretenimento

Solução

Akamai API Security

Akamai

criadas para oferecer o grau de visibilidade, segurança em tempo real e testes contínuos que as soluções de segurança de APIs especializadas podem oferecer. Grande parte dessas proteções não poderia ser trabalhada com a infraestrutura atual. Por exemplo, dois dos principais aspectos da segurança de APIs são autenticação e autorização. Mecanismos de autenticação adequados garantem que apenas usuários ou sistemas autorizados possam acessar as APIs.

Descoberta de vulnerabilidades

A equipe de segurança de APIs da Akamai usou seus módulos de gerenciamento de postura e proteção de tempo de execução para entender a postura atual de segurança de APIs do cliente. Depois que já tínhamos um inventário preciso das APIs no ambiente do cliente, pudemos descobrir quaisquer vulnerabilidades de segurança existentes e configurações incorretas.

A primeira descoberta foi que o cliente foi vítima de uma SQLi (injeção de linguagem de consulta estruturada). Uma SQLi é um tipo de vulnerabilidade de segurança que ocorre quando um invasor pode manipular os parâmetros de entrada de uma solicitação de API para executar comandos de SQL não autorizados. As consequências de um ataque de SQLi bem-sucedido podem ser graves. Os invasores podem obter acesso não autorizado a dados confidenciais, modificar ou excluir dados ou até mesmo executar comandos arbitrários no servidor de banco de dados subjacente.

A segunda descoberta foi que faltava autenticação para o cliente. Sem autenticação adequada, qualquer pessoa pode acessar os pontos de extremidade da API e potencialmente recuperar ou modificar dados confidenciais. Ela pode modificar ou excluir dados, gerando problemas de integridade de dados e uma perda potencial de informações críticas. Isso pode levar a violações de dados, divulgação não autorizada de informações, ou até mesmo comprometimento completo do sistema.

Perspectivas futuras

Agora que o cliente tem um controle firme sobre suas APIs em produção, ele vem explorando como lidar com vulnerabilidades antes da produção. Para ajudar as organizações a encontrarem e corrigirem essas vulnerabilidades, o Akamai API Security inclui o Active Testing, uma solução de teste de segurança de APIs criada especificamente para entender a lógica de negócios exclusiva de uma organização e fornecer cobertura abrangente de suas vulnerabilidades específicas de API. O Active Testing pode ajudar a organização a usar uma abordagem "shift-left" e estabelecer testes de segurança de APIs a todas as fases do desenvolvimento.

 | Publicado em 09/24