Akamai Customer Story

Sports and Media Company Uncovers Hidden API Risks

Building a full API inventory and uncovering misconfigurations that open doors to API attacks

Built accurate inventory | Spotted missing controls | Discovered SQL injection

Digital platforms and applications are revolutionizing the sports and media industry through the power of APIs. These technological advancements are transforming the way live events are organized, promoted, and experienced, creating new opportunities for artists, event organizers, and audiences alike.

APIs can seamlessly share event information, updates, and ticket links across various social media channels, increasing visibility and driving ticket sales. Moreover, APIs are transforming the on-site experience at live events. Integration with mobile applications and wearable devices enables interactive features such as personalized schedules, interactive maps, and real-time notifications.

It's important to note, however, that the sensitive nature of the data and transactions involved in the sports and media sector makes it imperative to prioritize API security. API security controls play a critical role in ensuring the integrity, confidentiality, and availability of data — which is why this world-renowned sports and media organization engaged Noname Security (now an Akamai company).

Adopting API security

The customer was well aware of the need for API security but wasn't exactly sure where they should start and which areas should be prioritized. Traditionally, they had been primarily focused on application security and felt that their existing tools, like API gateways and web application firewalls, would suffice in protecting APIs. However, while tools like these

Sports and Media Company

Location

United States

Industry

Media and Entertainment

Solution

Akamai API Security

Akamai

can offer certain baseline protections, they aren't designed to provide the degree of visibility, real-time security, and continuous testing that specialized API security solutions can provide. Much of these protections could not be addressed with their current infrastructure. For example, two of the key aspects of API security are authentication and authorization. Proper authentication mechanisms ensure that only authorized users or systems can access the APIs.

Uncovering vulnerabilities

The Akamai API Security team used its Posture Management and Runtime Protection modules to understand the customer's current API security posture. Once we had an accurate inventory of the APIs in the customer's environment, we were then able to uncover any existing security vulnerabilities and misconfigurations.

The first discovery was that the customer was a victim of a Structured Query Language injection (SQLi). A SQLi is a type of security vulnerability that occurs when an attacker can manipulate the input parameters of an API request to execute unauthorized SQL commands. The consequences of a successful SQLi attack can be severe. Attackers can gain unauthorized access to sensitive data, modify or delete data, or even execute arbitrary commands on the underlying database server.

The second discovery was that the customer was missing authentication. Without proper authentication, anyone can access API endpoints and potentially retrieve or modify sensitive data. They can modify or delete data, leading to data integrity issues and a potential loss of critical information. This can lead to data breaches, unauthorized information disclosure, or even complete system compromise.

Future outlook

Now that the customer has a firm grip on their APIs in production, they've been exploring how to address vulnerabilities before production. To help organizations find and remediate these vulnerabilities, Akamai API Security includes Active Testing, which is a purpose-built API security testing solution that can understand an organization's unique business logic and provide comprehensive coverage of their API-specific vulnerabilities. Active Testing can help the organization shift left and establish API security testing into every phase of development.

 | Published 09/24