

숨겨진 API 리스크를 발견한 스포츠 및 미디어 기업

전체 API 인벤토리 구축 및 API 공격의 문을 열어주는 잘못된 설정 발견



정확한 인벤토리 구축



누락된 제어 발견



SQL 인젝션(SQLi) 발견

디지털 플랫폼과 애플리케이션은 API를 활용해 스포츠 및 미디어 업계에 혁명을 일으키고 있습니다. 이러한 기술 발전은 라이브 이벤트의 준비, 홍보, 경험 방식을 변화시켜 아티스트, 이벤트 주최자, 관객 모두에게 새로운 기회를 창출하고 있습니다.

API는 다양한 소셜 미디어 채널에서 이벤트 정보, 업데이트, 티켓 링크를 원활하게 공유해 가시성을 높이고 티켓 판매를 촉진할 수 있습니다. 또한 API는 라이브 이벤트의 현장 경험을 변화시키고 있습니다. 모바일 애플리케이션 및 웨어러블 디바이스와의 통합 작업을 통해 개인 맞춤형 일정, 인터랙티브 지도, 실시간 알림과 같은 인터랙티브 기능을 사용할 수 있습니다.

그러나 스포츠 및 미디어 분야와 관련된 데이터와 거래의 민감한 특성으로 인해 **API 보안**을 우선시해야 합니다. API 보안 제어는 데이터의 무결성, 기밀성, 가용성을 보장하는 데 중요한 역할을 하기 때문에 세계적인 스포츠 및 미디어 기업은 Noname Security(현재 Akamai가 인수한 기업)와 계약을 체결했습니다.

API 보안 도입

해당 고객은 API 보안의 필요성은 잘 알고 있었지만 어디서부터 시작해야 할지, 어떤 영역에 우선순위를 두어야 할지 정확히 알지 못했습니다. 기존에는 주로 애플리케이션 보안에 중점을 두고 있었기 때문에 API 게이트웨이나 웹 애플리케이션 방화벽과 같은 기존 툴이 API를 충분히 보호한다고 생각했습니다. 그러나 이런 툴은 일부 보안 기능을 제공할 수는 있지만, 전문 API 보안 솔루션이 제공할 수 있는 수준의 가시성, 실시간



Sports and Media Company

위치
미국

업계
미디어 및
엔터테인먼트

솔루션
Akamai API Security



보안, 지속적인 테스트를 제공하도록 설계되지는 않았습니다. 이러한 보안 기능의 대부분은 고객의 현재 인프라로는 해결하기 어렵습니다. 예를 들어, API 보안의 핵심적인 두 가지 측면은 인증과 권한 부여입니다. 적절한 인증 메커니즘은 권한이 부여된 사용자 또는 시스템만 API에 접속할 수 있도록 보장합니다.

취약점 발견

Akamai API Security 팀은 체계 관리 및 런타임 보호 모듈을 사용해 고객의 현재 API 보안 체계를 파악했습니다. 고객 환경에 있는 API의 정확한 인벤토리를 확보한 후에는 기존의 보안 취약점과 잘못된 설정을 발견할 수 있었습니다.

첫 번째 발견은 고객이 구조화된 쿼리 언어 인젝션(SQLi)의 피해자였다는 것이었습니다. SQLi는 공격자가 API 요청의 입력 매개변수를 조작해 권한이 없는 SQL 명령을 실행할 때 발생하는 보안 취약점의 한 종류입니다. SQLi 공격이 성공하면 심각한 결과를 초래할 수 있습니다. 공격자는 민감한 데이터에 무단으로 접속하거나, 데이터를 수정 또는 삭제하거나, 기본 데이터베이스 서버에서 임의의 명령어를 실행할 수도 있습니다.

두 번째 발견은 고객이 인증을 누락하고 있다는 것이었습니다. 적절한 인증이 없으면 누구나 API 엔드포인트에 접속해 민감한 데이터를 검색하거나 수정할 수 있습니다. 데이터를 수정하거나 삭제할 수 있어 데이터 무결성 문제가 발생하고 중요한 정보가 손실될 가능성이 있습니다. 이는 **데이터 유출**, 무단 정보 공개 또는 전체 시스템 감염으로 이어질 수 있습니다.

향후 전망

이제 고객은 프로덕션 환경에서 API를 확실히 파악하고 있기 때문에 프로덕션 전에 취약점을 해결하는 방법을 모색하고 있습니다. Akamai API Security는 기업이 이런 취약점을 발견하고 해결할 수 있도록 하기 위해 기업의 고유한 비즈니스 로직을 이해하고 API별 취약점에 대한 포괄적인 커버리지를 제공하도록 특별히 설계된 API 보안 테스트 솔루션인 Active Testing을 제공합니다. Active Testing은 기업이 시프트 레프트(shift left)를 시행하고 모든 개발 단계에 API 보안 테스트를 도입하는 데 도움을 줄 수 있습니다.

