Kuipernet

API Security

보안 가이드

ASTSOFT

㈜에이에스티소프트

작성 이력

작성일	변경 내용
2024년 11월	API Security 보안 가이드

목 차

1. API Security 필요성

API Security 필요성

API 보안은 디지털 서비스 확산과 API의 급속한 증가로 인해 중요성이 커지고 있습니다.
특히 API는 애플리케이션 간 데이터와 기능을 주고받는 주요 경로로, 이를 통해 기업은 외부 파트너나 고객과 서비스를 원활하게 연계하고, 비즈니스 효율성을 높입니다.
하지만 이러한 개방성은 보안 위협을 증가시키며, API가 악용될 경우 데이터 유출이나 서비스 중단, 비즈니스 손실로 이어질 위험이 큽니다.

2. API Security 동향

API Security 동향

해외 시장은 이미 API 보안에 대해 주목하며 경각심을 불러일으키고 있다.
가트너(Gartner)에 따르면 “2022년부터 API 남용이 가장 빈번한 공격 경로로 대두돼 기업의 웹 애플리케이션 침해가 발생할 것”이라고 분석했다. 데이터 분석가 샤민 필라이(Shameen Pillai)는 “2024년까지 API 남용 및 관련 데이터 침해가 거의 두 배로 증가할 것”으로 예측했다. 또한 가트너는 “2025년까지 기업 API의 50%가 ‘관리되지 않은 상태’로 있을 것”이라고 진단했다. 포레스터(Forrester)는 “보안 의사결정권자(61%), LOB 의사결정권자(59%), 앱개발 의사결정권자(56%) 등 비즈니스 전반의 의사결정권자가 향후 12개월 동안 가장 중요한 보안 우선순위로 API를 꼽았다”며 “API 도입 증가에 따른 공격표면 확대·데이터 보안에 대한 두려움(55%), 민감한 데이터가 잘못된 사람에게 노출되는 것에 대한 두려움(52%)이 가장 큰 것으로 조사됐다”고 발표했다.
API 불안정과 관련된 비용도 증가하고 있다. 마시 맥레넌(Marsh McLennan) 사이버 리스크 분석 센터(Cyber Risk Analytics Center)의 ‘API 불안정 비용 정량화’ 연구에 따르면 API 불안정으로 인해 연간 410억~750억달러의 손실이 발생하는 것으로 분석됐다.
국내에선 마이데이터 기술 가이드라인 개정(개정일 2021년 11월 10일)에 따라 금융권의 API 보안이 의무화됐다. 이로 인해 보안의 중요성은 더욱 커지고 있다. API 보안이 중요한 이유는 기업은 API를 이용해 서비스를 연결하고, 데이터를 전송하기 때문에 API가 손상, 노출 또는 해킹되면 주요 데이터 유출 사고의 원인이 되기 때문이다. 더군다나 금융권은 이용자의 자산을 보호하고 있기에 금융정보와 이용자의 개인정보보호는 매우 중요하다.
하지만 금융권을 시작으로 API 보안을 점진적으로 확대 적용해야 한다는 보안전문가들의 의견과 달리, 기업의 API 보안은 여전히 뒷전이다.

Gartner의 설문조사에서

1. 70%의 기업이 디지털변환으로 API가 중요하다고 답변했습니다.
   디지털 혁신과 API보안을 가장 큰 과제로 꼽았습니다.
2. 94%의 기업이 third-parties가 제공하는 퍼블릭 API를 사용할 계획이라고 답했습니다.
3. 90%의 조직이 파트너가 제공하는 비공개 API를 사용할 계획이라고 답했습니다.
4. 80%의 조직이 공개적으로 노출된 API를 제공 할 계획이라고 답했습니다

3. API 공격 현황

API 공격 현황

Region	Weekly Impacted Organization	Change from Jan. 2023
North America	1 in 4.3	+39%
Latin America	1 in 4.4	+39%
Europe	1 in 4.5	+1%
APAC	1 in 4.7	+71%
Africa	1 in 4.9	+85%

기업 4곳 중 1곳이 2024년 첫 몇 달 동안 사이버 공격을 받았습니다.

4.API 주요 피해 사례

2-1. 아드하르(Aadhaar)

2-2. 링크드인(LinkedIn)

2-3. 전자상거래 JustDial

2-4. 페이스북(Facebook)

2-5. Uber의 API 인증 취약점 사건

2-6. T-Mobile API 공격

주요 피해 사례

2-1. 아드하르(Aadhaar)

분류	내용
사고날짜	2018年 1月
피해규모	약 11억 명의 신원/생체인증 정보 노출

2018년 초, 해커들이 세계 최대의 ID 데이터베이스인 아드하르에 잠입해 지문과 홍채 스캔과 같은 생체 데이터는 물론 이름, 주소, 사진, 전화번호, 이메일을 비롯한 11억 명 이상의 인도 국민에 대한 정보들을 노출했다는 뉴스가 나왔다.
아드하르의 데이터베이스(2009년 UIDAI(Unique Identification Authority of India)에서 구축)에는 고유한 12자리 숫자로 연결된 은행 계좌에 대한 정보가 포함되어 있기 때문에, 이는 신용 정보 유출이기도 했다. 불행하게도, 인데인의 API는 접근 제어가 없어서 데이터를 취약하게 만들었다.

주요 피해 사례

2-2. 링크드인(LinkedIn)

분류	내용
사고날짜	2021年 7月
피해규모	사용자 7억 명

2021년 6월 다크 웹 포럼에 7억 개의 링크드인 계정이 게시되어 사용자 기반 90% 이상에 영향을 미쳤다. 갓 유저(God User)라는 별명을 가진 해커는 약 5억 명의 고객이 있는 첫 번째 정보 데이터 세트를 버리기 전에 사이트의 API를 이용하여 데이터 스크래핑 기술을 사용했다. 그러고 나서 7억 개의 고객 데이터베이스를 모두 판매한다고 과시했다. 갓 유저가 게시한 스크래치 데이터 샘플에는 이메일 주소, 전화번호, 지리 위치 기록, 성별 및 기타 소셜 미디어 세부 정보를 포함한 정보가 들어 있었다.

주요 피해 사례

2-3. 전자상거래 JustDial

분류	내용
사고날짜	2019年
피해규모	약 1억 명

인도의 검색 엔진이자 소셜 마켓인 JustDial은 2019년에 고객 정보 데이터베이스를 공개한 혐의를 받았다. 1억 명이 넘는 사용자가 정보가 유출되면서 영향을 받았다. 이러한 정보에는 이메일, 이름, 전화번호, 생년월일, 직업 및 사진이 포함되어 있었고 사이트에 포함된 모든 사용자 정보가 노출되었다. 이 공격은 JustDial의 API 엔드포인트가 공개적으로 액세스 가능했기 때문에 발생했는데, 엔드포인트에는 보안이 전혀 없었고 액세스는 무제한 API를 통해 제공되어 이를 통해 데이터베이스에 액세스할 수 있는 사람은 누구나 원하는 정보를 얻을 수 있었다.

주요 피해 사례

2-4. 페이스북(Facebook)

분류	내용
사고날짜	2018年
피해규모	8,700만 명

페이스북은 타사 애플리케이션이 페이스북 사용자 데이터를 수집할 수 있도록 API를 제공해왔는데, 이 API가 보호되지 않아 외부 회사인 케임브리지 애널리티카(Cambridge Analytica)가 약 8,700만 명의 사용자 데이터를 무단으로 수집한 사건이 발생했다.
이는 사용자 동의 없이 수집된 데이터가 정치적 목적으로 사용된 사례로 큰 논란을 일으켰고, API 권한과 데이터 관리의 중요성을 다시금 일깨워 주었다.

주요 피해 사례

2-5. Uber의 API 인증 취약점 사건

분류	내용
사고날짜	2016年
피해규모	약 5,000만 명

우버는 API 인증 절차의 허점을 악용한 해커로 인해 사용자 정보가 유출된 바 있습니다. 인증이 충분히 보안되지 않아서, 해커는 사용자 계정 정보와 개인 데이터를 쉽게 접근할 수 있었으며, 결국 우버는 약 5천만 명의 사용자와 운전자의 데이터를 해커에게 탈취당했다. 이 사건은 API 호출에 대한 인증 및 권한 부여의 중요성을 강조하게 만든 대표적 사례이다.

주요 피해 사례

2-6. T-Mobile API 공격

분류	내용
사고날짜	2021年
피해규모	약 4,000만 명

미국의 통신사 T-Mobile은 API를 통한 공격으로 인해 약 4천만 명의 사용자 데이터가 노출된 사건이 있었다. 공격자는 API의 인증 우회 취약점을 이용해 사용자 정보에 접근했으며, 여기에는 고객의 사회 보장 번호(SSN), 이름, 생년월일 등의 민감한 정보도 포함되었다. 이 사건 이후 T-Mobile은 보안 프로토콜을 강화하고, API 호출에 대한 모니터링을 더욱 엄격히 진행하기 시작했다. T-Mobile은 가입자의 약 0.2%가 데이터 침해의 영향을 받았다고 생각하는데, 이는 약 200,000명의 영향을 받은 사용자에 해당하며, 이 공격의 결과로 T-Mobile의 주가는 6.3% 하락했다.

5. 금융보안원
금융API 보안 가이드

5-1. 금융보안원 금융권 Open API 보안 권고

5-2. 금융권 Open API 보안 강화 필요성

5-3. 금융권 Open API 구조와 보안 관리 대상

5-4. 각 주제별 주요 보안 리스크와 대응 방안

금융보안원 금융 API 보안 가이드

5-1. 금융보안원 금융권 Open API 보안 권고

금융권에서 오픈 API는 다양한 외부 서비스와 데이터를 안전하게 연동하여 금융 서비스를 확장하고 혁신을 지원하는 중요한 도구입니다. 그러나, 금융 데이터를 다루는 만큼 보안에 취약할 경우 심각한 리스크를 초래할 수 있습니다.
2018년 금융보안원에서 발표한 금융권 OPEN API 이용기관 자체 보안 점검 가이드를 발표하였습니다.

5-2. 금융권 Open API 보안 강화 필요성

고객 신뢰도 확보	외부 공격에 대한 방어	규제 및 컴플라이언스 준수
금융권에서 보안 사고는 고객 신뢰에 직접 영향을 미칩니다. 강력한 보안을 통해 고객 데이터와 자산을 안전하게 보호 함으로써 신뢰를 확보	금융 API가 외부에 개방되면 SQL 인젝션, 크리덴셜 스터핑 등 다양한 보안 공격에 노출되기 쉽습니다. 보안이 미흡한 경우 사용자 계정 탈취, 자산 탈취, 민감 데이터 유출과 같은 큰 피해가 발생할 수 있습니다.	금융 API는 개인정보 보호법, 금융 보안 관련 규제 준수 의무가 있으며, 규제 위반 시 막대한 법적 책임과 신뢰도 손실로 이어질 수 있습니다.

5-3. 금융권 오픈 API 구조와 보안 관리 대상

금융권에서 오픈 API 이용 구조는 크게 운영기관, 이용기관, 이용자 세 가지 영역으로 구분됩니다. 일반적으로 운영기관은 API 제공자(예: 은행)이며, 이용기관은 API를 이용하여 서비스를 제공하는 핀테크 기업 등이며, 이용자는 최종 고객입니다.
서비스 사용에 있어 주요 단계는 최초 서비스 등록 부분과 이후 서비스 이용에 있다.
각 단계별 절차상 보안 취약점이 있는지 “검토 → 확인 → 수정/보완 → 모니터링” 과정을 반복해야 한다.

5-4. 각 주제별 주요 보안 리스크와 대응 방안

구분	주요 리스크	보안 대책
이용자	이용자 계정 탈취, 개인정보 유출, 피싱 공격	다단계 인증(2FA), 강력한 비밀번호 정책, 피싱 사이트 방지
이용기관	인증 정보 관리 실패, API 트래픽 과다 발생, 시스템 오작동	사용자 교육, 다중 인증 기술 적용, API 접근 권한 관리 강화 Rate Limiting 설정, 실시간 모니터링, 트래픽 이상 감지 및 보고, API 이용 정책 준수
운영기관	API 오용, DDoS 공격, 데이터 조작	API 보안 제품을 통한 보안 강화, API의 악성 트래픽 필터링 및 로깅, 방화벽 및 API 모니터링 솔루션 적용, API 토큰의 제한된 만료 시간 설정

6. OWASP Top 10 API Security

OWASP Top 10 API Security

OWASP Top 10 API Security 2019	OWASP Top 10 API Security 2023
API1 Broken Object Level Authorization	API1 Broken Object Level Authorization 유지
API2 Broken User Authorization	API2 Broken Authorization 업데이트
API3 Excessive Data Exposure 통합(API3)	API3 Broken Object Property Level Authorization 업데이트
API4 Lack of Resources and Rate Limiting	API4 Unrestricted Resource Consumption 업데이트
API5 Broken Function Level Authorization	API5 Broken Function Level Authorization 유지
API6 Mass Assignment 통합(API3)	API6 Unrestricted Access to Sensitive Business Flows 신규
API7 Security Misconfiguration	API7 Server Side Request Forgery 신규
API8 Injection 삭제	API8 Security Misconfiguration 유지
API9 Improper Assets Management	API9 Improper Inventory Management 업데이트
API10 Insufficient Logging and Monitoring 삭제	API10Unsafe Consumption of APIs 신규