POINT OF VIEW

The Importance of API Security in Telecom Networks and Services

As telecoms seek to drive growth through service innovation to enterprise verticals and consumers, two types of APIs have emerged as anticipated means for innovation, agility, and monetization: compute (including edge) APIs and network APIs.

Compute APIs are a set of programming interfaces that allow developers and third parties to access and utilize edge platform resources, such as compute, storage, and networking used for running applications, services, and different tasks and value-add functionalities.

Network APIs have grown in presence and importance as telecom networks' programmability grew. These APIs have two main functions:

1. Real-time network information exposes network telemetry and can enhance network and service hygiene, fine-tune and customize services, and create monetization opportunities.
2. Network configuration allows application functions (AFs) to customize their network and service environment to drive service innovation and customization levels.

Internal and external API exposure delivers efficiency, agility, innovation, and monetization. At the same time, APIs are used as attack vectors, with recent successful API-based attacks in telecom operators has resulted in significant operational and financial impact. Securely exposing these APIs is, therefore, a key requirement focus for both telecoms operators and regulators alike.

APIs in Modern Telecom Networks

Compute and network API consumption span multiple domains and use cases, ranging from telemetry and integration to operations and management, all the way to service activation and delivery. These can be divided into four broad categories:

- **Customer and service management APIs** are usually powered by business-support platforms that enable customer and product management, service activation and life-cycle management, marketing and sales enablement, billing, payment support, and more.
- **Integration APIs** are heavily used as telecoms depend on partners for delivering, maintaining, and offering value-added services to customers that B2B APIs enable. These APIs enable partner onboarding, provide access to required data and internal services, and enable service management and revenue settlement.
- **Network exposure APIs** are used to deliver network information to and accept configuration requests from partners, customers, and third parties to enable service innovation, customization, and monetization based on specific use cases, customer requirements, and network behavior.
- **Shadow APIs** consist of forgotten, abandoned, or undocumented APIs. This group also includes a spectrum of accidentally exposed APIs from past test and preproduction environments.

API Attacks Are Happening

APIs are vulnerable to a range of threats from misconfigured and inadequate authentication and authorization, information disclosure, classical web attacks (such as command execution), local and remote file inclusion, as well as inadequate rate-limiting and denial-of-service (DoS) protection.

In the past few years, there have been several examples of API attacks gaining access to sensitive customer information that was then infiltrated in tier-1 operators in Europe, APAC, APAC, and North America.

Multilayer API Cybersecurity Is Required

To safeguard the complex and critical nature of API interworking in telecom networks, a multilayer cybersecurity approach is required, consisting of the following layers:

1. Centralized API authentication and authorization enforcement
2. Ensuring least-privilege access for AF clients
3. API requests validation to ensure requests conform to input and a set of predefined rules
4. Response filtering to avoid unwanted disclosure of sensitive information
5. Detection of vulnerabilities during the API and service life cycle (development and deployment)
6. Maintenance of an API inventory to track exposed APIs
7. Protecting against known and unknown API vulnerabilities and attacks
8. Protecting the underlying platforms

Comprehensive API Security with the Fortinet Security Fabric

As part of the Fortinet Security Fabric platform, a set of network and application cybersecurity tools offer the ability to protect APIs and their related services throughout their life cycle. These are provided via application-layer perimeter defense, underlying infrastructure security, AI-driven API security, and cybersecurity integration during the CI/CD life cycle. These tools provide a set of integrated and converged cybersecurity functionalities, management, and reporting, empowering telecoms to secure their API infrastructure, ecosystem, and monetization to drive agility, innovation, and growth.

June 9, 2023 11:40 PM

2197716-0-0-EN