Top API Security Risks Enterprises Need to Address

Every API expands the attack surface. Here are 10 risks enterprises cannot afford to overlook.

01 Broken Authorization

Attackers access data or functions beyond their permissions.

Risk: Unauthorized access • Privilege escalation

02 Broken Authentication

Weak credentials, tokens, or sessions enable user impersonation.

Risk: Account takeover • Unauthorized transactions

03 Excessive Data Exposure

APIs return sensitive data beyond what users actually need.

Risk: Data leakage • Privacy exposure

04 Unrestricted Resource Consumption

Abuse of requests or payloads can overwhelm API resources.

Risk: Downtime • Higher infrastructure costs

05 Injection Attacks

Malicious API inputs can manipulate databases or systems.

Risk: Data compromise • System manipulation

06 Security Misconfiguration

Weak CORS, default settings, exposed endpoints, and verbose errors create openings.

Risk: Larger attack surface • Information disclosure

07 Improper API Inventory

Shadow, legacy, and undocumented APIs can remain unsecured.

Risk: Unknown attack paths • Legacy vulnerabilities

08 Unsafe Third-Party Integrations

External APIs can introduce risks outside direct security controls.

Risk: Supply chain exposure • Cascading compromise

09 Insufficient Monitoring

Poor visibility can leave malicious API activity undetected.

Risk: Longer dwell time • Delayed response

10 Insecure Business Logic

Attackers exploit legitimate workflows, limits, or transaction logic.

Risk: Fraud • Business process abuse

www.ampcuscyber.com | letsconnect@ampcuscyber.com