wallarm

RESEARCH REPORT

Wallarm API ThreatStats™ Report Q3'2023

Executive Summary

Navigating the rapidly evolving realm of cybersecurity is crucial for the protection of critical digital resources. The Wallarm API ThreatStats™ Report for Q3'2023 underscores a surge in threats centered around APIs, necessitating urgent and concentrated efforts from business leaders and cybersecurity practitioners. The API ThreatStats™ report offers a detailed examination into the ever-changing threats targeting APIs, and uncovers critical vulnerabilities. It serves as an essential guide through this complex cyber landscape and provides expert insights and recommendations.

The Q3'2023 report introduces a revamped "Top 10 API Security Threats" compilation, a real-time data-driven list covering the **239 vulnerabilities** that were discovered in the quarter. What distinguishes Wallarm's methodology from traditional frameworks like OWASP is our unique approach and classification that specifically targets pressing vulnerabilities which are critical in today's modern API ecosystem. Recognizing these threats and their implications enables organizations to take immediate and proactive steps to strengthen their defenses and safeguard critical assets.s.

Persistent dangers, notably injections and the growing issue of API data leaks, take center stage in this quarter's report. Evidence of these risks is found in the recent serious data breaches suffered by leading firms including Netflix, VMware, and SAP. This underscores the essential role of API leak prevention within corporate security planning. It is evident that protecting against API leaks needs to be a central focus of any corporate security strategy, not an afterthought.

239

total API vulnerabilities identified in Q3'23

33%

of vulnerabilities linked to AAA issues

Key Recommendations

Limitations of Existing Frameworks and Benchmarks

While established frameworks like the OWASP API Security Top-10 provide an invaluable guideline and framework, it's important to recognize their limitations. They may not comprehensively address the expansive security needs of today's diverse API portfolio and infrastructure, and are not sufficient to prioritize security efforts. Wallarm's real-time data-driven threat list, which identifies severe threats and critical vulnerabilities not covered by static frameworks, should be an integral part of an overall security strategy.

Incorporating API Leak Protection Measures

API leaks have emerged as a significant threat, yet they are often overlooked. It is crucial to incorporate API leak protection measures into a security strategy program. Despite not being covered in the OWASP API Security guidelines, the Q3'2023 report highlights a multitude of incidents traced back to leaked credentials (including by 3rd parties) leading to security breaches. It is paramount to implement an automatic discovery system of leaked API keys and secrets, enforcing controls and measures to block their use, and protect against any subsequent attacks.

Prioritizing AAA Principles

The foundation of robust API security lies in the core principles of Authorization, Authentication, Access Control (referred to as AAA) and are fundamental to robust API security. It's essential to acknowledge these core principles are also subject to security issues and flaws that can have severe ramifications. The Q3'2023 report witnessed a surge in vulnerabilities related to AAA within technology stacks that are used by various technology companies. This underscores the necessity for organizations to regularly commit and update their entire security stack to effectively mitigate potential risks.

Don't Underestimate Traditional Vulnerabilities

Traditional app-level vulnerabilities are still a major threat. Based on our analysis, Injections are still the #1 issue, based on the sheer number of vulnerabilities. The fact that some incidents are not related to modern concerns like BOLA but to traditional legacy threats like CSRF, SSRF, or XSS doesn't diminish the severity of the problem.

Prepare for Reducing SLA Risks

Be prepared for the potential hazards and risks related to reduced Service Level Agreements (SLAs) as your APIs are susceptible to misuse and/or Distributed Denial-of-Service (DDoS) attacks. Certain API issues, including Logic Bombs and unsafe API resource consumption, can make it easier for attackers to disrupt service availability.

Snapshot of Top-10 API Security Risks in the Wallarm API ThreatStats™ Q3'2023 report

Rank #	Issues	Class Description
1	59	**Injections:** Encompasses a wide variety of attack vectors like SQL, XML, and Command Injections.
2	37	**Authentication Flaws:** Issues where identity verification fails.
3	30	**Cross-Site Issues:** Includes CSRF, XSS and other threats targeted across different sites.
4	26	**API Leaks:** Leaking sensitive information such as API Keys, JWT tokens, etc.
5	23	**Broken Access Control:** Access governance loopholes that may lead to unauthorized data exposure.
6	19	**Authorization Issues:** Lapses in resource access controls post-authentication.
7	15	**Unsafe Resource Consumption:** Server exhaustion and service disruptions.
8	13	**Weak Secrets and Cryptography:** Issues like hard-coded secrets or weak encryption algorithms.
9	9	**Sessions and Password Management:** Inadequate session handling and poor password management schemes.
10	7	**SSRF:** Server-Side Request Forgery attacks, distinct from injections.

For further information you can download the entire report by clicking here Wallarm API ThreatStats report Q3'2023. Feel free to reach out to our Wallarm security experts who can help to navigate and address your challenges.

(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107