wallarm

WALLARM.COM

Q2 2025

API ThreatStats Report

wallarm

Contents

Introduction

As the CEO of Wallarm, I have the unique vantage point of watching the API threat landscape evolve not in theory, but in real time, across some of the world’s most critical infrastructure. What we saw in Q2 2025 is not just an escalation, it's a shift in the very nature of how modern systems are being targeted.

This quarter’s Wallarm API ThreatStats Report is designed to provide clarity amid that shift. This report provides a structured, data backed view of the trends in API related CVEs, OWASP-aligned risks, public breach analyses supported by real-world exploitation trends and practical recommendations.

API threats escalated from a persistent concern to a systemic risk, exacerbated by the accelerating growth of AI and its reliance on API-driven architectures. Wallarm's analysis uncovered 639 unique CVEs directly tied to API vulnerabilities, many embedded in AI orchestration frameworks, DeOps pipelines, and cloud-native platforms. These are not edge cases but they sit at the core of how modern enterprises’ digital systems operate. This quarter also witnessed a continuation of high-impact API breaches at major organizations like Microsoft Azure, TeleMessage, and LangSmith, each reinforcing the reality that API exploits are not hypothetical but active, damaging and growing in sophistication.

As CEO of Wallarm, I believe it is our commitment to our customers and the industry to carefully track and analyze these critical developments.

Ivan Novikov
CEO and Co-founder

Executive Summary

APIs now form the nervous system of the digital enterprise powering AI orchestration, customer experiences, and cloud-native operations. But in Q2 2025, it became undeniably clear: APIs are also the fastest-growing attack vector.

The Q2 2025 API ThreatStats Report, powered by Wallarm Threat Intelligence, provides a comprehensive analysis of the evolving API threat landscape. It draws on data from over 600+ API-related CVEs, dozens of in-the-wild exploits tracked by CISA, and real-world breach incidents involving companies like Microsoft Azure, LangSmith, Wordpress, and TeleMessage, and more. The report connects vulnerabilities, exploitation techniques, and breach behaviors into a unified narrative and delivers clear, actionable guidance for security leaders and practitioners navigating this new threat surface.

More than just a snapshot of vulnerabilities, this report focuses on how APIs are being exploited, why traditional defenses are failing, and what defenders must do to stay ahead.

In this report, you will learn where today's API threats are truly coming from, backed by real exploit data, breach analysis, and CVE trends. You'll discover how attackers are shifting from traditional injection flaws to abusing business logic and misconfigured AI interfaces, and why static tools and legacy WAFs are no longer enough. Whether you're a CISO making board-level decisions or a practitioner defending production systems, this report equips you with the insights, examples, and prioritized actions needed to build resilient, runtime-ready API security in 2025 and beyond.

APIs are the fastest-growing attack vector in 2025, with 1000+ CVEs and breaches showing why traditional defenses fail and how to build resilient security.

API Threat Landscape

Powered by Wallarm Threat Intelligence

Q2 Spotlight

GraphQL: An Underestimated API Security Risk

GraphQL has revolutionized modern application development by addressing the limitations of traditional REST APIs. While it empowers developers with unmatched flexibility and efficiency, it also introduces unique security challenges that require unique capabilities.

There were no GraphQL-specific breaches reported in the Q2 2025 public data, so why are we highlighting it here? The widespread adoption of GraphQL particularly in AI interfaces, mobile backends, and enterprise SaaS demands preemptive attention. GraphQL's ability to reduce payload sizes by 99% compared to REST, combined with its dynamic, declarative, schema-driven structure, makes it ideal for data heavy applications. GraphQL's flexibility and client-driven data fetching offer performance gains, but also increase the risk of:

GraphQL is demonstrating strong market momentum and result for adopters. 70% of organizations are now using GraphQL.[1]

1 Overly broad data exposure (akin to API3: Broken Object Property Authorization)

2 Denial of Service via complex or nested queries (API4: Resource Consumption)

3 Authorization bypasses through improperly secured resolvers (API1 and API5)

4 Lack of visibility into shadow queries and custom operations

Why It Matters

Unlike REST, GraphQL allows a single endpoint to serve diverse and dynamic queries. This introduces blind spots for security teams who rely on path-based inspection, rate limiting, or static contract enforcement. As GraphQL adoption grows silently across tech stacks, attackers are already experimenting with introspection abuse, excessive query nesting, and injection attacks targeting poorly hardened resolvers.

[1] Migrating to GraphQL: A Practical Assessment

Strategic Takeaway

The absence of GraphQL breaches in Q2 2025 reporting does not indicate safety; it may signal a lack of detection and attribution. GraphQL has not traditionally been well supported by API security tools. Organizations using GraphQL should treat it as a unique class of API architecture requiring specialized protections:

- Disable or secure introspection in production.
- Enforce query cost analysis and depth limiting.
- Authenticate and authorize at the field and resolver level.
- Monitor query patterns for abnormal complexity or access attempts.

API Vulnerability Trends

The second quarter of 2025 saw a 9.8% increase in API-related CVEs compared to Q1, with 639 vulnerabilities disclosed between April and June up from 582 in Q1. This sharp rise reflects not only the growing volume of APIs in production but also the increased scrutiny and attacker interest in integration surfaces, especially those connected to AI workloads.

A major trend distinguishing Q2 from Q1 is the acceleration of AI-specific API vulnerabilities. Wallarm identified 34 CVEs tied directly to AI APIs this quarter up from just 19 in Q1. These primarily impacted model-serving endpoints, orchestration frameworks (like LangFlow and MLflow), and plugin ecosystems built atop platforms like OpenCV and Jenkins. This shift underscores how API security and AI security are becoming inseparably linked.

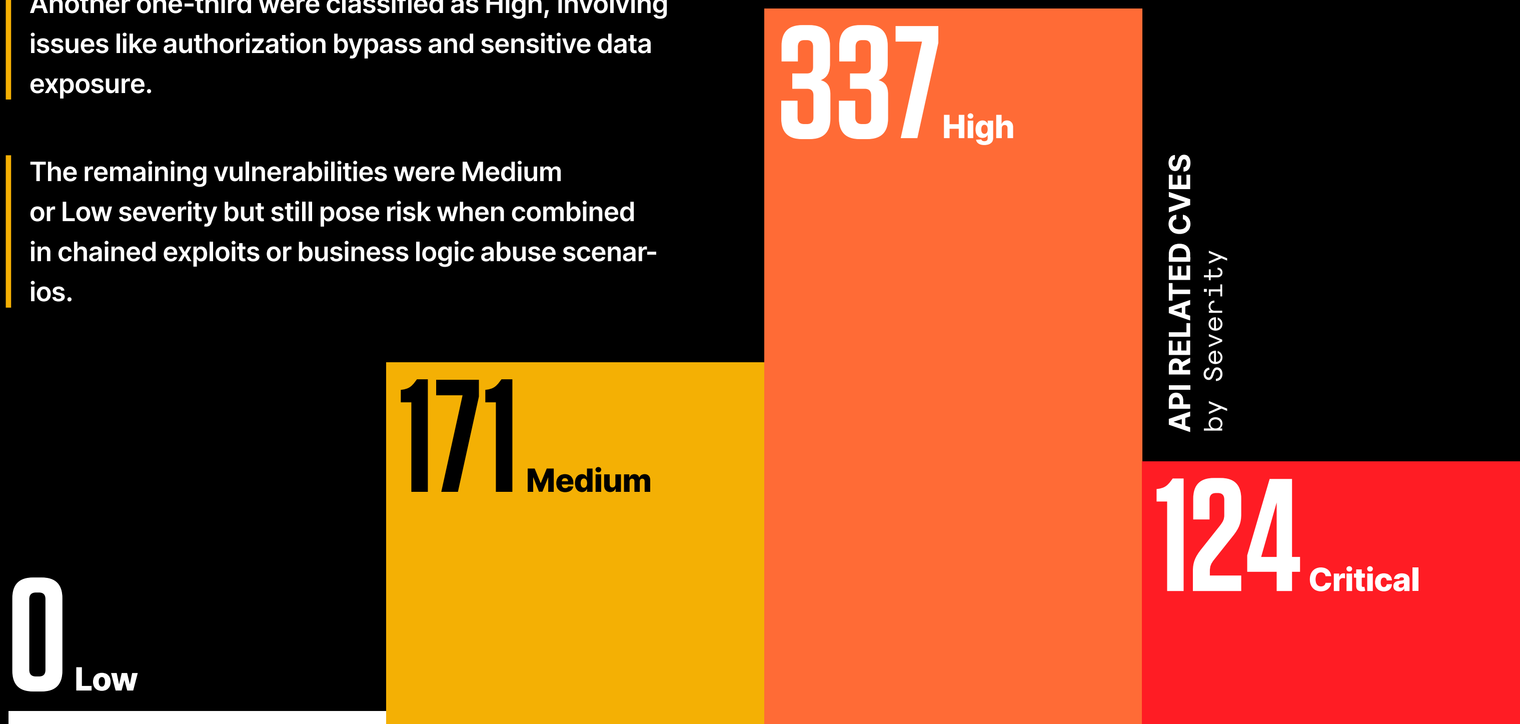
The severity distribution reveals that API vulnerabilities are not just increasing in volume but also in criticality:

> **Roughly one-third of all CVEs were Critical, typically enabling remote code execution, token leakage, or insecure deserialization.**

> **Another one-third were classified as High, involving issues like authorization bypass and sensitive data exposure.**

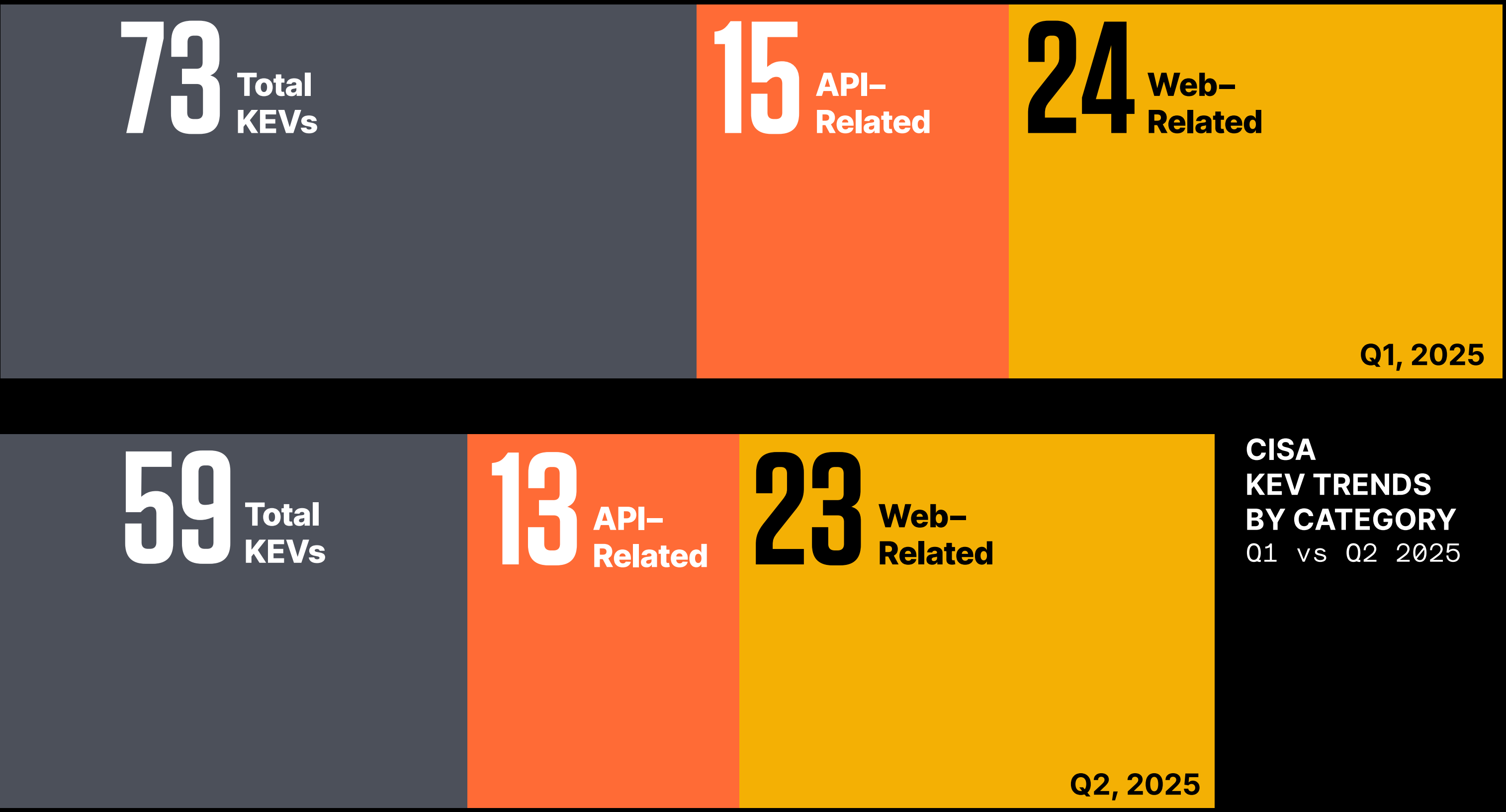
> **The remaining vulnerabilities were Medium or Low severity but still pose risk when combined in chained exploits or business logic abuse scenarios.**

The dominance of High and Critical severity CVEs in the dataset highlights the urgent need for proactive security especially in API-driven AI platforms, which are increasingly targeted due to their access to sensitive models, data, and decision logic. With AI-related APIs (e.g., Langflow, KYC tools) present in the dataset, the risk is amplified: a single flaw can expose proprietary algorithms or enable model manipulation. Prioritizing API security is essential to protect both infrastructure and AI integrity in modern applications.



API Exploit Trends

Between April 1 and June 30, 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) added 59 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog. Among them, 13 were directly API-related, representing 22% of all confirmed in-the-wild exploits for the quarter.



CISA KEV TRENDS BY CATEGORY
Q1 vs Q2 2025

As seen in the graphic, API-related vulnerabilities dropped slightly in count, from Q1 to Q2 2025, but they made up a larger share of all KEVs indicating that they remain a core target surface even in a slower quarter overall. This highlights a focus among attackers on exploiting APIs as initial access points, particularly through misconfigured endpoints, broken authorization, and exposed orchestration layers.

Common Exploitation Themes in Q2 API KEVs

1 **Unauthenticated Access Points**
Several API vulnerabilities exploited in the wild allowed access without requiring credentials highlighting the risks of exposed endpoints and default configurations.

2 **Broken Authorization**
A majority of API-related KEVs exploited BOLA (Broken Object Level Authorization), where APIs validated identity but failed to restrict object-level access.

3 **Token Abuse and Session Hijacking**
Some APIs exposed token mechanisms that could be reused or escalated to higher privileges.

4 **Injection and Execution Flaws**
KEVs involving GraphQL resolvers and shell-exposed endpoints revealed command injection or insufficient query sanitization.

> **Q2 exploits hit hard through open endpoints, broken auth, token abuse, and injections — proof that weak API design is an open door for attackers.**

The API-related KEVs from Q2 2025 reveal a troubling pattern of structural weaknesses in API design and deployment. Exploits frequently stemmed from unauthenticated access points and misconfigured endpoints, allowing attackers to bypass identity checks entirely. Broken Object Level Authorization (BOLA) flaws were widespread, enabling unauthorized access to sensitive data even when identity validation was in place. For enterprises, the business consequences are significant: these technical oversights can lead to large-scale data leaks, operational disruption, regulatory exposure, and erosion of customer trust. Addressing them requires a shift from reactive patching to proactive API governance, visibility, and runtime protection.

API Breaches

The second quarter of 2025 saw a continued rise in high-impact API breaches. We saw a series of significant breaches exposing systemic weaknesses in API security across diverse platforms, from AI-powered SaaS applications to core infrastructure services.The breaches observed reveal that attackers are increasingly exploiting a combination of misconfigurations, insufficient authentication controls, and unpatched vulnerabilities often in widely adopted components.

These incidents also highlight that the API attack surface extends beyond production business logic to include debug interfaces and AI agent integrations. In many cases, exploitation required nothing more than sending an HTTP request to an exposed endpoint, illustrating a dangerous gap between the complexity of modern systems and the maturity of their security controls. This reality demands that security teams rethink API defense strategies, ensuring controls are applied comprehensively across the full API lifecycle from design and deployment to storage and retirement. As usual we analyzed all the API-related breaches that occurred within the quarter. Through this analysis we have ranked and shared the top 5.

When the Guardians Slip: Lessons from the APISec Breach

The APISec breach is a stark reminder that even security-focused companies, whose core mission is to protect others, are not immune to lapses. In this case, a misconfigured, unprotected database exposed over three terabytes of sensitive customer information, including security scan results, credentials, and personal data. The fact that this occurred at a company specializing in API security illustrates a key lesson: no organization can assume immunity from basic security failures. Every system, whether labeled "test" or "production," must be treated as sensitive, with strict access controls, regular audits, and robust monitoring in place. Whether you're defending APIs, networks, or data stores, the same discipline applies continuous monitoring, proactive protection, and regular audits are a must.

Top 5 API Breaches Q2 2025

RANK	VENDOR	IMPACT	WHAT HAPPENED	WHY IT MATTERS
1	asana	**1,000+** customer projects	A vulnerability in Asana's MCP server software exposed data from Asana instances to other MCP users, with the data type being limited to each user's access scope.[1]	This shows that integrating AI features without rigorous testing can unintentionally expose sensitive customer data across organizations
2	LangSmith	High risk for compromised agent users	A malicious AI agent vulnerability in LangSmith's Prompt Hub let attackers embed hidden proxies to steal API keys, data, and tamper with LLM responses.[2]	AI agents can embed hidden data exfiltration paths, so they must be reviewed and tested before implementation
3	Microsoft Azure	**50,000** Azure AD users	An unsecured, unauthenticated JavaScript-embedded API endpoint issued Microsoft Graph tokens with elevated privileges, exposing sensitive data.[3]	Ensure proper authentication for API access in code, otherwise it will leave an open door for attackers
4	TeleMessage	**410 GB** government data	The root issue was a misconfigured Spring Boot Actuator /heapdump endpoint that was publicly accessible. This allowed a hacker to download a live heap dump of a snapshot of the server's memory.[4]	Even a single misconfiguration can instantly expose huge volumes of sensitive private data
5	Major Tech Service Provider	**30,000** employee records	An Unauthenticated API endpoint associated with the service provider's internal web application was exposed.[5]	Ensure proper audit of APIs. Leaving internal APIs open can lead to unintended consequences

[1] Asana Discloses Data Exposure Bug in MCP Server

[2] LangSmith Bug Could Expose OpenAI Keys and User Data via Malicious Agents

[3] 50,000+ Azure AD Users Exposed via Unsecured API: BeVigil Uncovers Critical Flaw

[4] TeleMessage Signal Clone Hack: Analysis and Implications

[5] Unprotected API Leaks Confidential Data of 33,000 Employee Records—BeVigil Raises the Alarm

Key Takeaways

Key Takeaways

Q2 2025 confirmed a strategic shift in the cybersecurity landscape: APIs are no longer a side concern, they are the primary attack vector. With 639 new API-related CVEs and multiple real-world breaches affecting millions of users, APIs are being exploited not through sophisticated zero-days, but through misconfigurations, missing access controls, and flawed logic.

From AI model orchestration to healthcare data exchange, APIs underpin the modern digital stack. Yet, their security often lags behind, with even mature organizations exposing debug endpoints, leaking tokens, and overlooking basic governance.

Unlike traditional exploits that breach from the outside in, API attacks start inside leveraging legitimate functionality and logic flaws. Threat actors are exploiting what was intentionally designed to work.

> **APIs have become the primary attack vector, exploited through misconfigurations, weak access controls, and logic flaws — turning core functionality into an entry point for attackers.**

Key Imperatives for Security Leaders & Practitioners

1 **Establish Full API Visibility**

You can't protect what you can't see. Continuously discover all APIs internal, external, AI-integrated, and shadow and enforce schema ownership and usage monitoring.

2 **Secure the AI Stack**

Audit every stage of your AI infrastructure from ingestion to inference. Disable default endpoints, enforce field-level access control, and monitor orchestration pipelines.

3 **Harden Authorization and Authentication**

Enforce granular access policies at every endpoint. Every major Q2 breach (APISec, LangSmith, Microsoft Azure) stemmed from exposed or under-protected APIs.

4 **Move Beyond Schema Checks**

Simulate real misuse: test for logic flaws, sequence abuse, and role escalation using behavior-based validation not just static contract enforcement.

5 **Shift Left and Secure Right**

Combine API security testing in development with inline runtime protection in production to cover the full API lifecycle.

The bottom line: API security is no longer just about preventing injections or following best practices. It's about treating APIs as critical assets that must be owned, governed, and monitored continuously. For both CISOs and practitioners, success now depends on proactive strategy, behavioral intelligence, and real-time control.

wallarm

Book a Demo

About Wallarm

Wallarm is the leading API security company, purpose-built to protect modern cloud-native and AI-driven architectures from today's most advanced threats. Our platform delivers complete visibility, intelligent threat detection, and real-time protection for all types of APIs like REST, GraphQL, gRPC, and increasingly, AI and Agent-based APIs.

As organizations adopt LLMs and autonomous agents, Wallarm helps secure the unique risks these interfaces introduce, including prompt injection, token abuse, and logic manipulation. By combining continuous API discovery, behavior-based analysis, and runtime policy enforcement, Wallarm enables security teams to protect complex API ecosystems including those powering AI without slowing innovation.

Learn more .... wallarm.com
Follow us .... Blog | X | LinkedIn | YouTube
Explore product .... tour.playground.wallarm.com

Secure APIs. Stop breaches.