

# THE RISE OF AGENT AI

API  
THREATSTATS™  
REPORT

Q1 2025

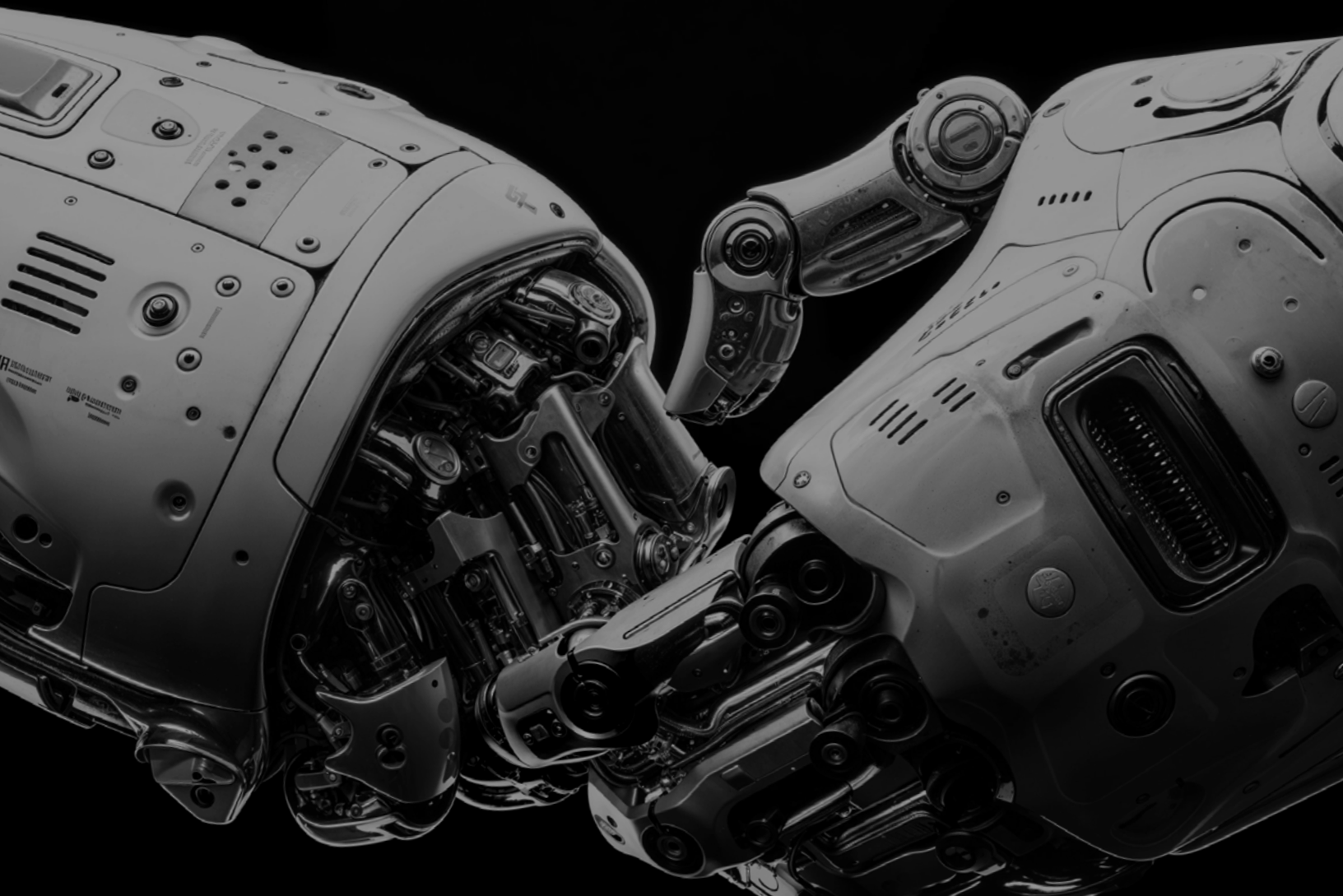


# Introduction

Welcome to the Wallarm API ThreatStats™ report for Q1 2025. These quarterly reports, and their annual counterpart, are designed to track the API threat landscape, identifying trends and changes. Our goal is to provide consistent assessment of how API threats are evolving so that practitioners can be better informed and more effectively defend their organizations.

In the first quarter of 2025, API threats continued to evolve rapidly, fueled by growing complexity in cloud-native infrastructure, the rise of agentic AI systems, and a surge in software supply chain risks.

Through this analysis, we'll uncover patterns and actionable insights that CISOs, security architects, and DevSecOps teams can use to prioritize risk and harden their defenses.



# Methodology

In order to produce this analysis, we've examined multiple datasets, using both AI and manual methods to classify conditions. The data includes:



## **CISA Known Exploited Vulnerabilities (KEV)**

The KEV catalog was reviewed in full, tagging vulnerabilities that are API related, and dividing them into modern and legacy APIs.



## **API Vulnerabilities**

We analyzed all published API-related vulnerabilities from Q1 2025. Each entry was mapped to OWASP and API-specific risk categories and scored using CVSS.



## **API Breaches**

The dataset includes nine incidents involving misconfigurations, hardcoded secrets, leaked API keys, and CVE exploitation.



## **Agentic AI GitHub Repositories**

New to the ThreatStats report this quarter, we analyzed 2,869 issues across agentic AI projects, filtering for API-relevant and security-related issues.

# Spotlight on Agentic AI Security

If you're reading this report and you're not aware of Agentic AI, you're in the minority. While the definition isn't always clear, we tend to label AI models and frameworks capable of autonomous task execution as Agents. And they present new security concerns, particularly around prompt injection, insecure API integrations, and hard-coded credentials.

APIs play a central role in all Agentic AI workflows, but the established cybersecurity standards like CVE and CISA KEV are trailing indicators of the API risk, and overall risk, presented by Agentic AI. In order to get ahead of the proverbial curve on Agentic AI security, we turned to GitHub. We chose to analyze GitHub security issues for Agentic AI repositories from October 2019 through March 2025, using some clever keyword filtering to identify them.

In fact, GitHub security data supports what we hypothesized, AI agent security risk largely stems from APIs. Of the 2,869 security issues analyzed in agentic AI projects, 1,858 (or 65%) were API-related, underscoring the inseparability of agent security and API security.

Our GitHub analysis revealed key patterns:

**1 858**  
ISSUES API-RELATED

**2 869**  
ISSUES TOTAL

## High Volume of API-Relevant Issues

1,858 of the 2,869 security issues were API-related.

**CWE-937**

Use of Unmaintained Code

**CWE-20**

Improper Input Validation

**CWE-400**

Uncontrolled Resource Consumption

**CWE-476**

NULL Pointer Dereference

**CWE-94**

Code Injection

**CWE-79**

Cross-site Scripting (XSS)

**CWE-200**

Exposure of Sensitive Information

**CWE-287**

Improper Authentication

**CWE-502**

Deserialization of Untrusted Data

**CWE-284**

Improper Access Control

## Security Issues by CWE (Common Weakness Enumeration)

The distribution of security issues in Agentic AI repositories by CWE serves as a roadmap to where we'll see issues in production deployments of AI agents. These weaknesses are likely to propagate into commercially developed agents. Organizations developing agents should proactively identify and address them, and organizations deploying agents should test for and defend against them.

**CWE-937** (Use of Unmaintained 3rd Party Components) topped the list. The high impact of 3rd party components on overall risk in AI agents mirrors software in general, but that doesn't make it any less of a risk.

**CWE-20** (Improper Input Validation) and **CWE-400** (Uncontrolled Resource Consumption) followed closely. These CWEs are prevalent in API risks in general, underlining how Agentic AI and API security are tightly coupled. Addressing the broader API security landscape benefits Agentic AI as well.



## Remediation Trends

The average time to close a security issue was 42 days, with many fixed within a week. However, some issues remained open for over 90 days, with the longest time to resolution being 1,284 days (approximately 3.5 years). Of the issues analyzed, 716 remain open, accounting for 25% of the total. It seems, not surprisingly, that active repositories are likely to address reported security issues quickly, while a significant percentage will simply ignore them.






It's clear from this data that agentic AI faces the same security challenges as other types of code. Furthermore, based on this data, AI agents are likely to have a large percentage of API-related vulnerabilities, making API security a clear requirement for Agentic AI security.

In fact, it's simply **not possible** to develop and deploy secure AI agents without API security.



# Top 5 API Breaches in Q1 2025

As usual, we analyzed all the API-related breaches that occurred within the quarter. There were a total of 9 qualifying incidents in Q1 2025. Through this analysis, we've ranked and shared the top 5.

RANK	VENDOR	IMPACT	WHAT HAPPENED	WHY IT MATTERS
1	 Oracle Cloud	<b>6M</b> Records	An attacker claimed to have exploited CVE-2021-35587, a vulnerability in Oracle Cloud's log-in infrastructure to access keys and passwords. <sup>1</sup>	This breach shows how a previously known CVE—present in the wild for years—can still lead to massive compromise if patching is incomplete. Oracle Cloud's size amplified the impact significantly.
2	 Deepseek	<b>1M+</b> Records Incident #1	A publicly accessible database disclosed API secrets. <sup>2</sup>	Highlights the importance of database access control, especially when sensitive API keys or secrets are exposed without authentication.
3	 Common Crawl	<b>11 908</b> Live Secrets	Common Crawl, a dataset used to train LLMs, was found to contain thousands of live API secrets. <sup>3</sup>	This breach draws attention to insecure software development practices, particularly around how secrets are managed and stored.
4	 Volkswagen	<b>800K</b> records	A weak JWT implementation allowed API access to user and vehicle data. <sup>4</sup>	Illustrates how a misconfigured API can expose sensitive customer information, even in large, security-conscious enterprises.
5	 NHS UK	Undisclosed	NHS patience data was exposed by Medefer via an unauthenticated API. <sup>5</sup>	The breach underscores the risks associated with aging infrastructure in critical sectors like healthcare, where legacy APIs are often overlooked.

1 <https://orca.security/>

2 <https://www.wiz.io/>

3 <https://cybersecuritynews.com/>

4 <https://media.ccc.de/>

5 <https://www.computerweekly.com/>

## Insight

Breaches tied to misconfiguration, hardcoded secrets, and unauthenticated API access dominated this quarter—particularly in AI and health-care sectors.

The horizontal nature of API security is evident in the breach data. APIs are everywhere, and so we see breaches across multiple industries, from healthcare to AI and beyond. API security isn't a challenge restricted to specific industry segments.

Honorable mention goes to Microsoft, BeyondTrust, and OmniGPT who all experienced incidents in the quarter as well, but didn't make the cut for the Top Five.





# API Vulnerability Trends

The vulnerability landscape for APIs in Q1 2025 was shaped by classic access control issues and newer risks introduced by cloud-native and AI-powered systems. First, some overall stats:

## Volume

# 582

API-related vulnerabilities were disclosed in Q1.

## Severity

# 7.42

The average CVSS score was 7.42



20

Uncontrolled Resource Consumption

CWE-400

Improper Authorization

CWE-285

Information Exposure

CWE-200

Improper Access Control

CWE-284

Improper Authentication

CWE-287

Improper Limitation of a Pathname  
to a Restricted Directory ('Path Traversal')

CWE-22

Improper Neutralization of Input During Web Page  
Generation ('Cross-site Scripting')

CWE-79

Improper Neutralization of Special Elements used  
in an SQL Command ('SQL Injection')

CWE-89

Cross-Site Request Forgery (CSRF)

CWE-352

Unrestricted Upload of File with Dangerous Type

CWE-434

Server-Side Request Forgery (SSRF)

CWE-918

## Top 11 CWE categories by CVE count

It's 11 because of the tie for spot number 10.

We analyzed the distribution of CVEs across Common Weakness Enumeration (CWE) categories. Uncontrolled Resource Consumption (CWE-400) took the top spot with 60 CVEs, but 60% of the top 5 were access control related, showing that access control issues remain prevalent across APIs.

150

100

50

200

API5

Broken Access Control

API2

Authentication Flaws

API7

Insecure Resource Consumptions

API1

Injections

API4

API Leaks

API3

Cross-site Issues

API10

SSRF

API8

Weak Secrets and Cryptography

API6

Authorization Issues

API9

Sessions and Password Management

## Count of CVEs by API ThreatStats™ Top 10 Category

We also analyzed the distribution of CVEs across the Wallarm API ThreatStats™ Top 10 categories, providing a more API-centric viewpoint on the root causes of these vulnerabilities. This analysis pushes the access control issues to the top, with **API5: Broken Access Control** netting 209 vulnerabilities. **API2: Authentication Flaws** came in at spot number 2 and **API7: Insecure Resource Consumption** came in third. The analysis shows that there is no overlap between CVEs categorized at CWE-400 and API5. In fact, API5 represents an aggregation of multiple access control related CVEs.

The vulnerability trends show that while there are a variety of security issues in APIs, access control (authentication and authorization) top the list as a category, followed by resource consumption issues.

# Conclusion

The data from Q1 2025 reinforces that APIs are not just part of the attack surface — they are the attack surface. From legacy system exposures to AI-native risks like hardcoded keys and injection vulnerabilities, attackers are targeting APIs as both the entry point and the objective.

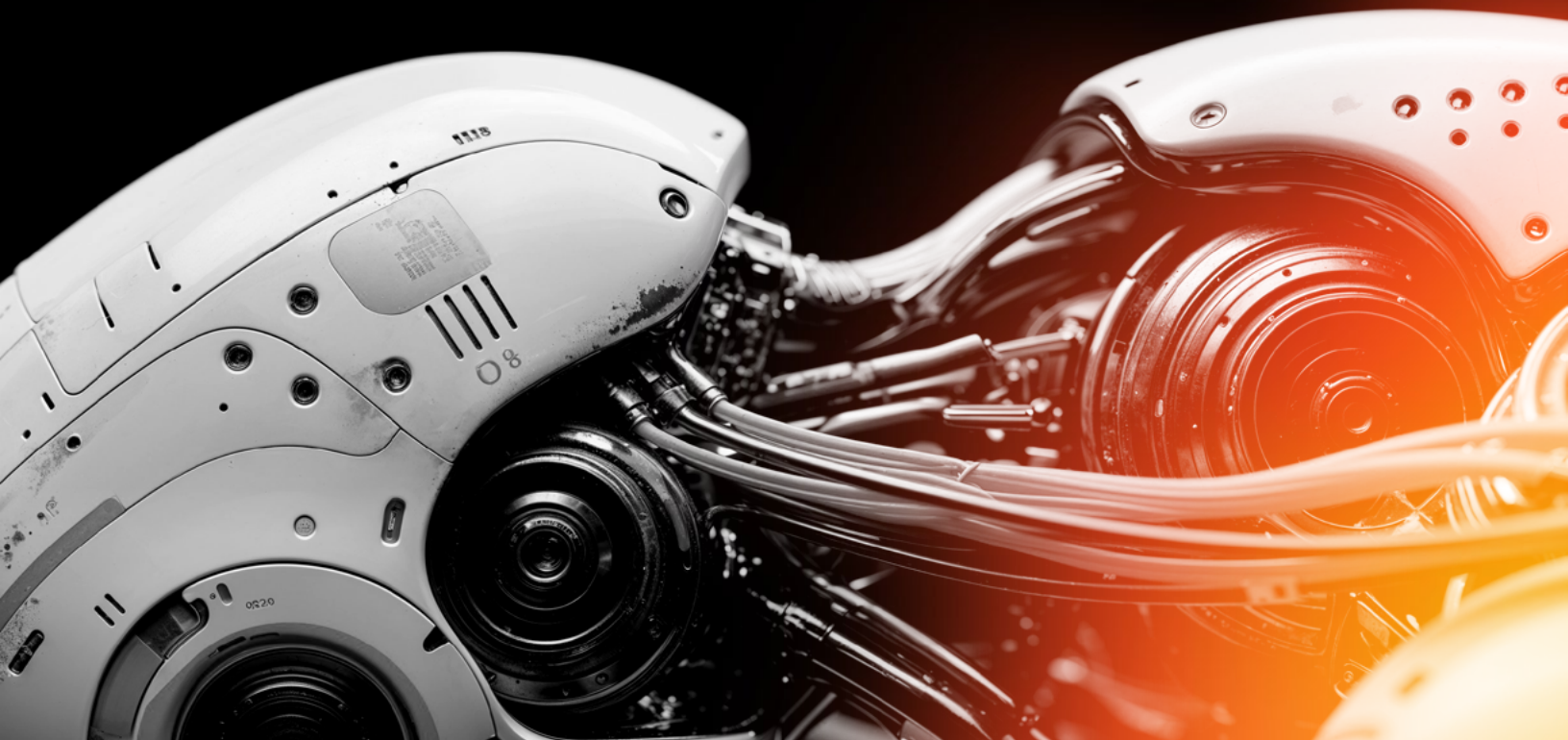
## Key Takeaways

**1 Agentic AI = New API Threat Frontier**  
Security issues in AI agent repositories on GitHub are widespread, API-heavy, and under-remediated. With an average fix time of 42 days, and many unfixed issues, they pose long-lived risks in production environments.

**2 Top API Breach Causes**  
Misconfiguration, hardcoded secrets, and unauthenticated access are recurring breach drivers. As usual, practitioners need to address new threats without forgetting about the existing threats that are still prevalent.

**3 Threat Type Trends**  
Access control is where it's at! The dominant vulnerabilities center on access control, authentication, and data exposure.

**4 Mitigation Momentum**  
With 15 API-related CVEs added to the CISA KEV list this quarter, the trend of API vulnerabilities dominating the exploit landscape continues.





## Action for CISOs

- 1 Update API threat models quarterly**  
Ensure that your existing threat models account for the current threat environment, including changes in your environment.
- 2 Create a security strategy for Agentic AI**  
The agents are coming, and now is the time to define your security strategy for agentic AI, including securing all the APIs to which those agents will connect.
- 3 Prioritize API security investments**  
Allocate resources to tools and training that specifically address API security, including real-time blocking, automated testing, and monitoring solutions.
- 4 Establish clear API security policies**  
Develop and enforce policies for secure API design, development, and deployment, including authentication, authorization, and data protection.

## Action for Practitioners

- 1 Update Security Workflows**  
Integrate CISA KEV data, third-party API issue exposure, and AI-specific risks into security workflows to stay ahead of evolving threats.
- 2 Monitor API traffic for anomalies**  
Implement real-time monitoring and blocking to stop malicious API activity, such as unauthorized access or data exfiltration.
- 3 Update your Threat Intelligence**  
Add new data feeds, such as [API ThreatStats](#), to your threat intelligence data.
- 4 Update Your API Discovery Methodology**  
If you're not already doing API Discovery, then you should start. If you are, then make sure you're also discovering those AI APIs.



# About Wallarm

Wallarm is the only unified platform for API and agentic AI security successfully deployed in enterprise production environments. Wallarm was founded to protect APIs, and has built a market leading platform for API protection, including API discovery, API abuse prevention, and AI protection. With Wallarm, customers receive the fastest, easiest, and most effective way to stop API attacks.

Organizations choose Wallarm to protect their APIs and AI agents because the platform delivers a complete inventory of APIs, real-time blocking, and patented AI/ML-based abuse detection. The Wallarm platform is built for modern tech stacks, and supports the deployment options that organizations need today. Wallarm supports full SaaS, hybrid, and on-premise deployments. The platform

detects and blocks API attacks across legacy and modern API protocols, including REST, gRPC, GraphQL, SOAP, Websockets, XML-RPC, and more.

Wallarm is headquartered in San Francisco, California, and is backed by Toba Capital, Y Combinator, Partech, and other investors.

Learn more.....[wallarm.com](https://wallarm.com)

Follow us.....[Blog](#) | [X](#) | [LinkedIn](#) | [YouTube](#)

Explore product.....[tour.playground.wallarm.com](https://tour.playground.wallarm.com)

© 2025 Wallarm, Inc. All rights reserved.

**WALLARM: SECURE APIS.  
STOP BREACHES.**